

Henkilötietojen suoja rikosasian käsittelyssä ja kansallista turvallisuutta ylläpidettäessä

Tietosuojadirektiivityöryhmän mietintö

Mietintöjä ja lausuntoja 52/2017

Henkilötietojen suoja rikosasian käsittelyssä ja kansallista turvallisuutta ylläpidettäessä

Tietosuojadirektiivityöryhmän mietintö



Oikeusministeriö

ISSN: 1798-7091 (nid.)

ISBN: 978-952-259-644-4 (nid.)

ISSN: 1798-7105 (PDF)

ISBN: 978-952-259-645-1 (PDF)

Helsinki 2017

Kuvailulehti

Julkaisija	Oikeusministeriö	25.10.2017	
Tekijät	Työryhmä; pj lainsäädäntöneuvos Timo Makkonen, sihteerit erityisasiantuntija Tanja Jaatinen, rajavartiolaitarkastaja Anne Ihanus, ylitarkastaja Virpi Koivu, ylitarkastaja Jaana Vehmaskoski, hallitussihteeri Perttu Wasenius		
Julkaisun nimi	Henkilötietojen suoja rikosasian käsittelyssä ja kansallista turvallisuutta ylläpidettäessä Tietosuojadirektiivityöryhmän mietintö		
Julkaisusarjan nimi ja numero	Oikeusministeriön julkaisu 52/2017		
Diaari/hankenumero	OM 21/41/2016 OM005:00/2017	Teema	Mietintöjä ja lausuntoja
ISBN painettu	978-952-259-644-4	ISSN painettu	1798-7091
ISBN PDF	978-952-259-645-1	ISSN PDF	1798-7105
URN-osoite	http://urn.fi/URN:ISBN:978-952-259-645-1		
Sivumäärä	208	Kieli	suomi
Asiasanat	henkilötietojen suoja, tietosuoja, työryhmät		
<p>Tiivistelmä</p> <p>Euroopan parlamentti ja neuvosto antoivat huhtikuussa 2016 direktiivin (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaitten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.</p> <p>Oikeusministeriö asetti tammikuussa 2017 työryhmän, jonka tehtävänä oli laatia ehdotus rikosasioiden tietosuojadirektiivin kansallista täytäntöönpanoa koskevaksi yleiseksi lainsäädännöksi samoin kuin ehdotukset direktiivin edellyttämistä muutoksista oikeusministeriön hallinnonalan lainsäädäntöön. Työryhmän tuli myös selvittää, voidaanko po. yleistä lainsäädäntöä soveltaa sellaiseen toimintaan, joka jää tietosuojadirektiivin ja tietosuoja-asetuksen soveltamisalan ulkopuolelle, mutta jonka sääntely on perusteltua sovittaa yhteen turvallisuusviranomaisia koskevan muun sääntelyn kanssa.</p> <p>Työryhmä ehdottaa, että direktiivin kansalliseksi täytäntöönpanemiseksi säädetään laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Työryhmä ehdottaa, että lakia sovellettaisiin myös Puolustusvoimien, poliisin ja Rajavartiolaitoksen käsitellessä henkilötietoja kansallisen turvallisuuden ylläpitämisen yhteydessä. Tältä osin kyse olisi kansallisesta ratkaisusta. Työryhmä ehdottaa tehtävän myös eräitä muutoksia oikeusministeriön toimialan lainsäädäntöön direktiivin täytäntöönpanemiseksi sen hallinnonalalla.</p> <p>Työryhmä ehdottaa, että ehdotettu lainsäädäntö tulisi voimaan 6 päivänä toukokuuta 2018.</p>			
Kustantaja	Oikeusministeriö		
Painopaikka ja vuosi	Lönnberg Print & Promo, 2017		
Julkaisun myynti/jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi		

Presentationsblad

Utgivare	Justitieministeriet		25.10.2017
Författare	Arbetsgruppen; ordf. lagstiftningsråd Timo Makkonen, sekreterare specialsakkunnig Tanja Jaatinen, gränsbevakningsöverinspektör Anne Ihanus, överinspektör Virpi Koivu, överinspektör Jaana Vehmaskoski, regeringssekreterare Perttu Wasenius		
Publikationens titel	Skydd av personuppgifter vid behandling av brottmål och upprätthållande av den nationella säkerheten Betänkande av arbetsgruppen för genomförandet av dataskyddsdirektivet		
Publikationsseriens namn och nummer	Justitieministeriets publikation 52/2017		
Diarie- /projektnummer	OM 21/41/2016 OM005:00/2017	Tema	Betänkanden och utlåtanden
ISBN tryckt	9978-952-259-644-4	ISSN tryckt	1798-7091
ISBN PDF	978-952-259-645-1	ISSN PDF	1798-7105
URN-adress	http://urn.fi/URN:ISBN:978-952-259-645-1		
Sidantal	208	Språk	finska
Nyckelord	skydd av personuppgifter, dataskydd, arbetsgrupper		

Referat

Europaparlamentet och rådet utfärdade i april 2016 direktivet (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

Justitieministeriet tillsatte i januari 2017 en arbetsgrupp för att bereda ett förslag till allmän lagstiftning om det nationella genomförandet av direktivet om dataskydd i brottmål samt förslag till sådana ändringar av lagstiftningen inom justitieministeriets förvaltningsområde som direktivet förutsätter. Arbetsgruppen skulle även utreda om den allmänna lagstiftningen i fråga kan tillämpas på sådan verksamhet som faller utanför dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde, men vars reglering det är motiverat att förena med den övriga regleringen gällande säkerhetsmyndigheter.

Arbetsgruppen föreslår att det för att genomföra direktivet på nationell nivå stiftas en lag om behandling av personuppgifter i brottmål och upprätthållande av den nationella säkerheten. Arbetsgruppen föreslår att lagen även tillämpas när Försvarsmakten, polisen och Gränsbevakningsväsendet behandlar personuppgifter i samband med upprätthållande av den nationella säkerheten. I detta avseende är det fråga om en nationell lösning. Arbetsgruppen föreslår även vissa ändringar i lagstiftningen inom justitieministeriets förvaltningsområde i syfte att genomföra direktivet inom detta förvaltningsområde.

Arbetsgruppen föreslår att den föreslagna lagstiftningen ska träda i kraft den 6 maj 2018.

Förläggare	Justitieministeriet
Tryckort och år	Lönnberg Print & Promo, 2017
Beställningar/ distribution	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Sisältö

OIKEUSMINISTERIÖLLE.....	9
ESITYKSEN PÄÄASIALLINEN SISÄLTÖ	13
YLEISPERUSTELUT	14
1 Johdanto	14
2 Rikosasioiden tietosuojadirektiivi.....	16
2.1 Yleistä	16
2.2 Rikosasioiden tietosuojadirektiivin pääasiallinen sisältö	16
3 Nykytila	24
3.1 Suomen lainsäädäntö ja käytäntö.....	24
3.2 Kansainväliset velvoitteet.....	31
3.2.1 EU:n lainsäädäntö.....	31
3.2.2 Kansainväliset sopimukset.....	32
3.2.3 Ulkomaiden lainsäädäntö.....	33
3.2.4 Kolmansien valtioiden kanssa tehdyt sopimukset	33
4 Nykytilan arviointi	34
5 Tavoitteet ja keskeiset ehdotukset	35
5.1 Tavoitteet	35
5.2 Keskeiset ehdotukset.....	35
6 Esityksen vaikutukset.....	44
6.1 Taloudelliset vaikutukset.....	44

6.2	Vaikutukset viranomaisten toimintaan	47
6.3	Yhteiskunnalliset vaikutukset	48
7	Asian valmistelu	49
8	Riippuvuus muista esityksistä	50
	YKSITYISKOHTAISET PERUSTELUT	52
9	Lakiehdotusten perustelut.....	52
9.1	Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä.....	52
9.2	Rikosrekisterilaki	102
9.3	Laki rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä.....	102
9.4	Laki oikeushallinnon valtakunnallisesta tietojärjestelmästä	103
9.5	Laki sakon täytäntöönpanosta	103
9.6	Laki henkilötietojen käsittelystä Rikosseuraamuslaitoksessa	104
9.7	Ulosottokaari	105
10	Voimaantulo.....	106
11	Suhde perustuslakiin ja säätämisyjärjestys	107
	LAKIEHDOTUKSET	111
	RINNAKKAISTEKSTIT	149
	LAGFÖRSLAG.....	158
	PARALLELLTEXT	197

OIKEUSMINISTERIÖLLE

Euroopan parlamentti ja neuvosto antoivat huhtikuussa 2016 osana Euroopan unionin tietosuojalainsäädännön uudistusta direktiivin (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäättöksen 2008/977/YOS kumoamisesta (jäljempänä *rikosasioiden tietosuojadirektiivi*). Rikosasioiden tietosuojadirektiivi on pantava kansallisesti täytäntöön 6.5.2018 mennessä.

Oikeusministeriö asetti 12.1.2017 työryhmän valmistelemaan ehdotuksen tarpeelliseksi yleiseksi lainsäädännöksi rikosasioiden tietosuojadirektiivin täytäntöön panemiseksi samoin kuin ehdotukset direktiivin edellyttämistä muutoksista oikeusministeriön hallinnonalan lainsäädäntöön. Työryhmän tuli lisäksi selvittää, voidaanko edellä mainittua yleistä lainsäädäntöä soveltaa sellaiseen toimintaan, joka jää rikosasioiden tietosuojadirektiivin sekä yleisen tietosuoja-asetuksen (EU) 2016/679 soveltamisalan ulkopuolelle, mutta jonka sääntely on perusteltua sovittaa yhteen turvallisuusviranomaisia koskevan muun sääntelyn kanssa.

Työryhmän tuli laatia ehdotuksensa hallituksen esityksen muotoon. Työryhmän toimikausi oli 16.1.–29.9.2017.

Työryhmän puheenjohtajaksi nimettiin lainsäädäntöneuvos Timo Makkonen oikeusministeriöstä.

Työryhmän jäseniksi kutsuttiin tietosuojavaltuutettu Reijo Aarnio, hallitusneuvos Anne Hartoneva oikeusministeriöstä, valtiosyyttäjä Johanna Hervonen Valtakunnansyyttäjänvirastosta, rajavartiolaitarkastaja Anne Ihanus sisäministeriöstä, hallitusneuvos Kari Liede oikeusministeriöstä, rekisteripäällikkö Teemu Mikkola Oikeusrekisterikeskuksesta, hallitussihteeri Taina Neira oikeusministeriöstä, erityisasiantuntija Tiina Nuutinen sisäministeriöstä, erikoissuunnittelija Ari Pajuniemi oikeusministeriöstä, neuvotteleva virkamies Leena Rantalankila oikeusministeriöstä, erityisasiantuntija Mirja Salo-

nen oikeusministeriöstä, hallitussihteeri Perttu Wasenius puolustusministeriöstä sekä neuvotteleva virkamies Jere Lumme valtiovarainministeriöstä.

Työryhmän sihteeiksi määrättiin oikeusministeriöstä erityisasiantuntija Tanja Jaatinen, neuvotteleva virkamies Leena Rantalankila sekä erityisasiantuntija Mirja Salonen, sisäministeriöstä ylitarkastajat Virpi Koivu ja Anne Ihanus, puolustusministeriöstä hallitussihteeri Perttu Wasenius ja valtiovarainministeriöstä neuvotteleva virkamies Jere Lumme.

Jere Lumpeen tilalle nimettiin työryhmän jäseneksi ja sihteeriksi 15.8.2017 alkaen ylitarkastaja Jaana Vehmaskoski. Rantalankila toimi tehtävässään toukokuun 2017 loppuun saakka ja Salonen kesäkuun 2017 loppuun saakka.

Työryhmä kokoontui toimikautensa aikana 12 kertaa.

Työryhmä ehdottaa, että säädetään uusi laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Kyseessä olisi yleislaki, jonka sääntelystä voitaisiin erityislainsäädännössä poiketa.

Lakia sovellettaisiin poliisin, syyttäjien, tuomioistuinten, Tullin, rajavontaviranomaisten ja muiden toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kysymys on rikoksen ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta, rikokseen liittyvistä syytetoimista, rikosasian käsittelemisestä tuomioistuimessa, rikosoikeudellisen seuraamuksen täytäntöönpanemisesta taikka yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä. Työryhmä ehdottaa lisäksi, että lakia sovellettaisiin myös Puolustusvoimien, poliisin ja Rajavartiolaitoksen käsitellessä henkilötietoja kansallisen turvallisuuden ylläpitämisen yhteydessä. Tältä osin kyse olisi kansallisesta ratkaisusta, sillä direktiivi ja yleinen tietosuoja-asetus eivät tule sovellettavaksi näissä tilanteissa.

Työryhmä ehdottaa myös eräitä direktiivin kansalliseen täytäntöönpanoon liittyviä tarkistuksia oikeusministeriön hallinnonalan lainsäädäntöön. Näitä tarkistuksia on valmisteltu oikeusministeriön palveluksessa olevien työryhmän jäsenten johdolla. Kyseistä lainsäädäntöä saatetaan eräiltä osin joutua arviomaan direktiivin näkökulmasta uudelleen siinä yhteydessä, kun lainsäädännön yhteensopivuutta yleisen tietosuoja-asetuksen kannalta myöhemmänä ajankohtana arvioidaan.

Saatuaan työnsä valmiiksi työryhmä luovuttaa kunnioittavasti mietintönsä oikeusministeriölle.

Helsingissä 28 päivänä syyskuuta 2017



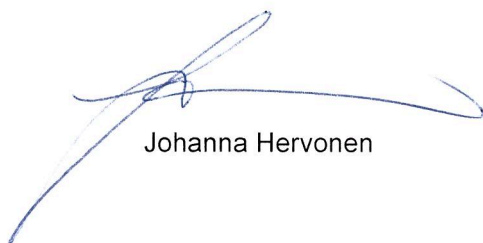
Timo Makkonen



Reijo Aarnio



Anne Hartoneva



Johanna Hervonen



Anne Ihanus



Virpi Koivu



Kari Liede



Teemu Mikkola



Taina Neira



Tiina Nuutinen



Ari Pajuniemi



Jaana Vehmaskoski



Perttu Wasenius



Tanja Jaatinen

Ehdotus hallituksen esitykseksi eduskunnalle henkilötietojen käsittelyä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä koskevaksi laiksi ja eräiksi siihen liittyviksi laeiksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Lailla pantaisiin täytäntöön Euroopan parlamentin ja neuvoston direktiivi luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.

Ehdotettua lakia sovellettaisiin poliisin, syyttäjien, tuomioistuinten, Tullin, Rajavartiolaitoksen ja muiden toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kysymys on rikoksen ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta, rikokseen liittyvästä syyttäjän toiminnasta, rikosasian käsittelemisestä tuomioistuimessa, rikosoikeudellisen seuraamuksen täytäntöönpanemisesta taikka yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä. Lakia sovellettaisiin myös puolustusvoimien, poliisin ja Rajavartiolaitoksen käsitellessä henkilötietoja kansallisen turvallisuuden ylläpitämisen yhteydessä. Tältä osin kyse on kansallisesta ratkaisusta.

Kyse olisi edellä mainituissa tilanteissa sovellettavasta yleislaista, jonka sääntelystä voidaan erityislainsäädännössä poiketa.

Ehdotetussa laissa säädettäisiin käyttötarkoitussidonnaisuudesta ja muista henkilötietojen käsittelyn yleisistä periaatteista, rekisterinpitäjän ja henkilötietojen käsittelijän vastuusta, tarkastusoikeudesta ja muista rekisteröidyn oikeuksista, tietoturvasuovaatimuksista, tietosuojavastaavan nimeämisestä ja tehtävistä, vaatimuksista siirrettäessä henkilötietoja kolmansiin maihin, lain noudattamisen valvonnasta sekä käytävissä olevista oikeusturvakeinoista ja seuraamuksista.

Lain noudattamista valvoisi Tietosuojavirasto.

Esityksessä ehdotetaan lisäksi eräitä muutoksia oikeusministeriön toimialan lainsäädäntöön rikosasioiden tietosuojadirektiivin täytäntöönpanemiseksi sen hallinnonalalla.

Lait ovat tarkoitetut tulemaan voimaan 6 päivänä toukokuuta 2018.

YLEISPERUSTELUT

1 Johdanto

Esityksen tarkoituksena on panna täytäntöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäättöksen 2008/977/YOS kumoamisesta (jäljempänä *rikosasioiden tietosuojadirektiivi* tai *direktiivi*). Direktiivi tuli voimaan 5 päivänä toukokuuta 2016 ja se on pantava täytäntöön 6 päivään toukokuuta 2018 mennessä.

Euroopan parlamentti ja neuvosto antoivat samanaikaisesti rikosasioiden tietosuojadirektiivin kanssa myös asetuksen (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (jäljempänä *yleinen tietosuoja-asetus*). Direktiivi ja asetus muodostavat yhdessä niin sanotun tietosuoja-paketin, jonka tarkoituksena on uudistaa voimassa oleva EU:n tietosuojalainsäädäntö. Yleinen tietosuoja-asetus on sellaisenaan jäsenvaltioissa sovellettavaa oikeutta, ja sitä aletaan soveltaa 25 päivänä toukokuuta 2018. Yleistä tietosuoja-asetusta on tarkoitus täydentää Suomessa kansallisella lainsäädännöllä, jota on valmisteltu erikseen.

Voimassa oleva EU:n tietosuojalainsäädäntö koostuu vuonna 1995 hyväksytystä direktiivistä (Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, jatkossa *henkilötietodirektiivi*) sekä rikosasioita koskevasta oikeudellisesta yhteistyöstä ja poliisiyhteistyöstä vuonna 2008 annetusta puitepäättöksestä (Neuvoston puitepäättös 2008/977/YOS, tehty 27 päivänä marraskuuta 2008, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta, jatkossa *puitepäättös*).

Tietosuojapaketin tavoitteena on päivittää ja nykyaikaistaa aikaisempaan henkilötietodirektiiviin sekä puitepäättökseen sisältyneet periaatteet, ottaen erityisesti huomioon

informaatioteknologian nopea kehitys sekä jatkuvasti kasvava henkilötietojen käsittelyn määrä. Uudistuksen erityisenä sisällöllisenä tavoitteena on parantaa rekisteröityjen oikeuksia, vahvistaa EU:n sisämarkkinoita, varmistaa henkilötietojen suojan korkea taso rikosasioita käsiteltäessä ja yhteiskunnassa muutoinkin, varmistaa tietosuojasääntelyn noudattaminen ja valvonta sekä edistää henkilötietojen liikkuvuutta.

Henkilötietodirektiivi on Suomessa pantu täytäntöön pääasiassa henkilötietolailla (523/1999). Sen lisäksi voimassa olevassa lainsäädännössä on huomattavan paljon tietosuojaa koskevaa erityissääntelyä. Rikosasioiden henkilötietodirektiivin sääntely on voimassa olevaa kansallista yleislainsäädäntöä selvästi yksityiskohtaisempaa ja osin siitä poikkeavaa, minkä lisäksi henkilötietolaki on tarkoitus kumota yleistä tietosuoja-asetusta täydentävällä kansallisella lainsäädännöllä. Edellä mainituista syistä esityksessä ehdotetaan uuden henkilötietojen käsittelyä rikosasioissa koskevan lain säätämistä.

Rikosasioiden tietosuojadirektiivi sen enempää kuin yleinen tietosuoja-asetuskaan eivät soveltamisalasäännöstensä perusteella tule sovellettavaksi sellaiseen henkilötietojen käsittelyyn, jota suoritetaan unionin oikeuden soveltamisalaan kuulumattoman toiminnan yhteydessä. Niiden soveltamisen ulkopuolelle jää muun muassa kansallisen turvallisuuden takaamisen yhteydessä suoritettu henkilötietojen käsittely. Jotta henkilötietojen käsittely tulee Suomessa kattavasti säännellyksi, ehdotettua lakia sovellettaisiin myös puolustusvoimien, poliisin ja Rajavartiolaitoksen käsitellessä henkilötietoja kansallisen turvallisuuden ylläpitämisen yhteydessä.

2 Rikosasioiden tietosuojadirektiivi

2.1 Yleistä

Euroopan komissio antoi ehdotuksensa yleiseksi tietosuoja-asetukseksi ja rikosasioiden tietosuojadirektiiviksi 27 päivänä tammikuuta 2012. Komission aloitteet perustuvat laajoihin, vuosina 2009–2011 järjestettyihin kuulemiskierroksiin sekä vaikutustenarviointiin. Direktiivi- ja asetusehdotuksia käsiteltiin neuvostossa samanaikaisesti.

Rikosasioiden tietosuojadirektiivin tarkoituksena on varmistaa henkilötietojen suoja direktiivin soveltamisalalla sekä helpottaa tietojen vapaata liikkuvuutta jäsenvaltioiden poliisi- ja oikeusviranomaisten välillä. Se on osittain luonteeltaan niin sanottu minimidirektiivi, koska sillä ei estetä jäsenvaltioita säätämästä korkeammasta rekisteröidyn oikeuksien suojan tasosta.

Rikosasioiden tietosuojadirektiivi kumoaa EU:n tietosuojapuitepäättöksen 2008/977/YOS 6 päivästä toukokuuta 2018 lukien. Molempien säädösten tarkoituksena on taata luonnollisten henkilöiden korkeatasoinen ja johdonmukainen suoja henkilötietojen käsittelyssä rikosasioissa sekä helpottaa henkilötietojen vaihtoa jäsenvaltioiden toimivaltaisten viranomaisten kesken. Kumottava puitepäättös koskee kuitenkin vain EU:n jäsenvaltioiden rajat ylittävää henkilötietojen käsittelyä, kun taas tietosuoja-direktiivi koskee myös jäsenvaltion sisällä tapahtuvaa henkilötietojen käsittelyä. Lisäksi tietosuojadirektiivi on yksityiskohtaisempi ja soveltamisalaltaan laajempi kuin tietosuojapuitepäättös, ja sisältää sitä vähemmän poikkeamismahdollisuuksia.

2.2 Rikosasioiden tietosuojadirektiivin pääasiallinen sisältö

Rikosasioiden tietosuojadirektiivissä on yhdeksän lukua. Luvut käsittelevät yleisiä säännöksiä, periaatteita, rekisterinpitäjää ja henkilötietojen käsittelijää, henkilötietojen siirtoja kolmansiin maihin tai kansainvälisille järjestöille, riippumattomia valvontaviranomaisia, yhteistyötä, oikeussuojakeinoja, vastuuta ja seuraamuksia, direktiivin täytäntöönpanoa sekä direktiivin loppusäännöksiä.

Yleiset säännökset

Direktiivin soveltamisala määritellään sen 2 artiklassa. Direktiiviä sovelletaan toimivaltaisten viranomaisten suorittamaan henkilötietojen käsittelyyn, kun kyse on rikosten ennalta estämisestä, tutkimisesta, paljastamisesta tai rikoksiin liittyvistä syytetoimista tai rikosoikeudellisten seuraamusten täytäntöönpanosta. Direktiiviä sovelletaan myös, kun kyse on yleiseen turvallisuuteen kohdistuvilta uhkilta suojelusta tai tällaisten uhkien ehkäisemisestä. Direktiiviä ei kuitenkaan sovelleta henkilötietojen käsittelyyn, jota suoritetaan unionin oikeuden soveltamisalaan kuulumattoman toiminnan yhteydessä tai jota suorittavat unionin toimielimet, elimet ja laitokset. Direktiivin soveltamisalan ulkopuolelle jää siten muun muassa Europolin ja Eurojustin toiminta sekä kansallinen turvallisuus ja puolustus. Soveltamisalarajoituksestaan huolimatta direktiivi mahdollistaa kansallisesti direktiivin mukaisen sääntelyn ulottamisen henkilötietojen käsittelyyn kansalliseen turvallisuuden ja puolustuksen alalla.

Direktiivin 3 artiklassa määritellään muun muassa henkilötietojen, käsittelyn, toimivaltaisen viranomaisen, rekisterinpitäjän, vastaanottajan ja kansainvälisen järjestön käsitteet. Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (*rekisteröity*) liittyviä tietoja. Toimivaltaisella viranomaisella tarkoitetaan kaikkia viranomaisia, joiden toimivalta kattaa rikosten ennalta estämisen, tutkimisen, paljastamisen tai rikoksiin liittyvät syytetoimet tai rikosoikeudellisten seuraamusten täytäntöönpanon. Toimivaltaisen viranomaisen käsite ulotetaan määritelmässä koskemaan myös sellaisia muita elimiä tai yksiköitä, joille on lailla annettu tehtäväksi käyttää julkista valtaa tai valtuuksia jossakin edellä mainitussa tarkoituksessa.

Periaatteet

Direktiivin 4–11 artiklassa säädetään henkilötietojen käsittelyä koskevista yleisistä periaatteista.

Jäsenvaltioiden on 4 artiklan mukaan säädettävä muun muassa siitä, että henkilötietoja käsitellään lainmukaisesti ja että niitä kerätään tiettyjä nimenomaisia ja laillisia tarkoituksia varten, eikä niitä käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Saman tai toisen rekisterinpitäjän suorittama käsittely muuta kuin alkuperäistä tarkoitusta varten on kuitenkin sallittua, jos käsittelystä säädetään laissa ja käsittely tätä muuta tarkoitusta varten on tarpeellista ja oikeasuhtaista. Artiklan 3 kohdassa on arkistointia sekä tieteellistä, tilastollista tai historiallista käsittelyä koskevat erityissäännökset. Käsittelyn lainmukaisuuden vaatimusta täsmennetään direktiivin 8 artiklassa, jonka mukaan käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin se on tarpeen toimivaltaisen viranomaisen tehtävän suorittamiseksi direktiivin soveltamisalalla ja jos se perustuu lakiin.

Eri ryhmiin, kuten rikoksista tuomittuihin ja rikoksen uhreihin, kuuluvien henkilötiedot on 6 artiklassa säädetyn mukaisesti tarvittaessa ja mahdollisuuksien mukaan selvästi erotettava toisistaan. Myös tosiseikkoihin perustuvat tiedot on mahdollisuuksien mukaan erotettava henkilökohtaisiin arvioihin perustuvista henkilötiedoista (7 artikla).

Direktiivin 10 artiklassa on säännökset erityisiä henkilötietoryhmiä koskevasta käsittelystä. Erityisillä henkilötietoryhmillä tarkoitetaan tietoja, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus taikka ammattiin liittyvä jäsenyys samoin kuin geneettisiä tietoja, biometrisiä tietoja sekä terveyttä taikka seksuaalista suuntautumista tai seksuaalista käyttäytymistä koskevia tietoja. Direktiivin 11 artiklassa on säännökset profiloinnista, mukaan lukien kielto käyttää sellaista profilointia, joka johtaa erityisiin henkilötietoryhmiin perustuvaan luonnollisten henkilöiden syrjintään. Direktiivi edellyttää myös tietoturvan ja tietojen laadun varmistamista.

Rekisteröidyn oikeudet

Direktiivin 12–18 artiklassa säädetään jäsenvaltioilta edellytetyistä lainsäädäntötoimenpiteistä rekisteröidyn oikeuksien turvaamiseksi.

Direktiivin 13 artiklassa edellytetään, että rekisterinpitäjän on asetettava rekisteröidyn saataville muun muassa rekisterinpitäjän henkilöllisyyttä, henkilötietojen käsittelyn tarkoitusta ja mahdollista tietosuojavastaavaa koskevat tiedot, samoin kuin tieto rekisteröidyn oikeudesta pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten henkilötietojen oikaisemista tai poistamista tai henkilötietojen käsittelyn rajoittamista.

Direktiivin 14 artiklassa säädetyn mukaan rekisteröidyllä tulee olla oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö häntä koskevia henkilötietoja. Rekisteröidyllä tulee myös olla oikeus saada pääsy henkilötietoihin sekä oikeus saada tiedot muun muassa käsittelyn tarkoituksista ja oikeusperusteesta. Direktiivin 16 artiklassa säädetyn mukaisesti rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan rekisteröityä koskevat virheelliset henkilötiedot. Direktiivi mahdollistaa sen, että rekisteröidyn oikeuksia voidaan käyttää välillisesti tietosuojaviranomaisten välityksellä.

Jäsenvaltiot voivat kuitenkin säätää oikeudesta rajoittaa edellä mainittujen tietojen antamista tai velvollisuutta henkilötietojen oikaisemiseen, jos se on välttämätöntä virallisten menettelyjen estämisen välttämiseksi, rikosten ennalta estämisen, paljastamisen, tutkimisen, syytetoimien tai rikosoikeudellisten seuraamusten täytäntöönpanon turvaamiseksi, yleisen turvallisuuden suojelemiseksi, kansallisen turvallisuuden suojelemiseksi taikka muiden henkilöiden oikeuksien ja vapauksien suojaamiseksi (13 artiklan 3 kohta, 15 artikla, 16 artiklan 4 kohta).

Rekisterinpitäjä ja henkilötietojen käsittelijä

Direktiivin 19–34 artiklassa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän vastuusta, henkilötietojen turvallisuudesta ja tietosuojavastaavasta.

Direktiivin 19 artiklassa säädetyn mukaisesti rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet sen varmistamiseksi ja osoittamiseksi, että käsittely vastaa direktiivissä säädettyjä vaatimuksia. Tällaisiin toimenpiteisiin on ryhdyttävä erityisesti sen varmistamiseksi, että tarvittavat henkilötietojen suojatoimet saadaan sisällytettyä käsittelyn osaksi (ns. sisäänrakennettu tietosuoja, 20 artiklan 1 kohta) ja että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja (ns. oletusarvoinen tietosuoja, 20 artiklan 2 kohta).

Direktiivin 21 artiklassa on keskinäistä vastuunjakoa koskevat säännökset tilanteista, joissa vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, jolloin ne katsotaan yhteisiksi rekisterinpitäjiksi.

Henkilötietojen käsittelyä ulkoistettaessa saa rekisterinpitäjä käyttää ainoastaan sellaista henkilötietojen käsittelijää, joka antaa riittävät takeet edellä mainittujen teknisten ja organisatoristen toimenpiteiden toteuttamisesta (22 artiklan 1 kohta). Rekisterinpitäjän ja henkilötietojen käsittelijän tulee laatia sopimus tai tehdä muu oikeustoimi, jossa vahvistetaan muun muassa käsittelyn kohde, kesto, luonne ja tarkoitus (22 artiklan 3 kohta).

Rekisterinpitäjän ja henkilötietojen käsittelijän on ylläpidettävä selostetta vastuulleen kuuluvista käsittelytoimista. Selosteen sisällöstä on otettu tarkemmat säännökset 24 artiklaan.

Automatisoiduissa käsittelyjärjestelmissä on säilytettävä 25 artiklassa tarkoitetut lokitiedot. Tiedot on säilytettävä seuraavista käsittelytoimista: tietojen kerääminen, muuttaminen, kysely, luovuttaminen siirrot mukaan lukien, yhdistäminen ja poistaminen. Kyselyjä ja luovutuksia koskevien lokitietojen avulla on pystyttävä toteamaan kyseisten toimien perusteet, toteutuspäivä ja -aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys. Lokitietoja saa käyttää ainoastaan käsittelyn lainmukaisuuden tarkistamiseen, omaehtoiseen valvontaan, henkilötietojen eheyden ja turvallisuuden varmistamiseen sekä rikosoikeudellisiin menettelyihin.

Direktiivin 27 artiklaan on otettu säännökset rekisterinpitäjän velvollisuudesta tehdä tietosuoja koskeva vaikutustenarviointi. Arviointi on tehtävä, jos tietäntyyppinen käsittely todennäköisesti aiheuttaa käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean

riskin. Jos kyseessä on uusi, tekeillä oleva rekisteri, ja vaikutustenarviointi osoittaa käsittelyn aiheuttavan korkean riskin jollei rekisterinpitäjä toteuta toimenpiteitä riskin lieventämiseksi, on valvontaviranomaista kuultava ennen henkilötietojen käsittelyn aloittamista (28 artikla). Valvontaviranomaista on kuultava myös, jos tietojen käsittely on sen luonteista, että siihen sisältyy muutoin rekisteröityjen oikeuksien ja vapauksien kannalta korkea riski, esimerkiksi uusien tekniikoiden, mekanismien tai menettelyjen käytön johdosta.

Direktiivin 29 artiklassa on säännökset rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudesta teknisin ja organisatorisin toimenpitein toteuttaa asianmukainen tietoturvallisuuden taso. Automatisoidun käsittelyn osalta niiden on esimerkiksi toteutettava toimenpiteet, joiden tarkoituksena on evätä asiattomilta pääsy käsittelyyn käytettäviin laitteisiin, estää tietovälineiden luvaton lukeminen sekä varmistaa, että automatisoidun käsittelyjärjestelmän käyttöön oikeutetut henkilöt pääsevät ainoastaan valtuutuksensa piiriin kuuluvien henkilötietoihin.

Henkilötietojen tietoturvaloukkauksen tapauksessa rekisterinpitäjä tulee ilmoittaa siitä valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta (30 artikla). Henkilötietojen käsittelijän on puolestaan ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle.

Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta myös rekisteröidylle, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietyin edellytyksin loukkauksesta ei kuitenkaan tarvitse ilmoittaa rekisteröidylle, muun muassa jos rekisterinpitäjä on toteuttanut jatko-toimenpiteitä, joilla varmistetaan, että edellä mainittujen riskien toteutuminen on epätodennäköistä. Rekisteröidylle ilmoittamista voidaan viivästyttää tai rajoittaa tai se voidaan jättää tekemättä, jos se on välttämätöntä virallisten menettelyjen estämisen välttämiseksi, rikosten ennalta estämisen, paljastamisen, tutkimisen, syytetoimien tai rikosoikeudellisten seuraamusten täytäntöönpanon turvaamiseksi, yleisen turvallisuuden suojelemiseksi, kansallisen turvallisuuden suojelemiseksi taikka muiden henkilöiden oikeuksien ja vapauksien suojaamiseksi.

Jäsenvaltioiden on säädettävä siitä, että rekisterinpitäjä nimittää tietosuojavastaavan. Jäsenvaltiot voivat vapauttaa tuomioistuimet ja muut riippumattomat oikeusviranomaiset tästä velvoitteesta näiden hoitaessa lainkäyttötehtäviään. Tietosuojavastaavan nimittämisestä, asemasta ja tehtävistä säädetään direktiivin 32–34 artiklassa.

Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille

Direktiivin 35–38 artiklassa on säännökset niistä edellytyksistä, joiden täytyessä henkilötietoja saa siirtää kolmanteen maahan tai kansainväliselle järjestölle. Siirron on

ensinnäkin oltava tarpeen kolmannen maan toimivaltaisten viranomaisten hoitaessa rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa koskevia tehtäviään. Tietoja voidaan siirtää vain sellaiseen kolmanteen maahan, jonka osalta Euroopan komissio on tehnyt tietosuojan riittävyyttä koskevan päätöksen. Jos komissio ei ole tehnyt tällaista päätöstä kyseisen maan osalta, tiedon siirtäminen edellyttää sopimusta henkilötietojen suojaamiseksi tehtävistä toimenpiteistä tai sitä, että rekisterinpitäjä kattavan arvion tehtyään katsoo henkilötietojen suojaamiseksi toteutetun asianmukaiset suojatoimet. Sekä komission päätöksen että asianmukaisten suojatoimien puuttuessa henkilötietoja saa siirtää vain eräistä erittäin painavista syistä, kuten luonnollisen henkilön elintärkeiden etujen suojaamiseksi tai jonkin maan yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhkan ehkäisemiseksi.

Riippumattomat valvontaviranomaiset

Jokaisella jäsenvaltiolla on oltava vähintään yksi riippumaton viranomainen, joka vastaa direktiivissä säädettyjen oikeuksien valvonnasta kyseisessä maassa. Tämä valvontaviranomainen voi olla sama kuin se, joka valvoo yleisen tietosuoja-asetuksen noudattamista kyseisessä maassa (41 ja 45 artikla). Valvontaviranomaisen on oltava riippumaton (42 artikla). Sen toimivaltaan ei kuitenkaan kuulu valvoa sellaisia käsitteilytoimia, joita tuomioistuimet suorittavat lainkäyttötehtäviensä yhteydessä.

Direktiivin 46 artiklassa säädetyn mukaisesti valvontaviranomainen käsittelee ja tutkii sille tehtyjä direktiivissä säädettyjen oikeuksien noudattamista koskevia valituksia. Valvontatehtävänsä ohella riippumattomalla viranomaisella on laajoja edistämisen, neuvonta-, lausunnonanto- ja yhteistyötehtäviä (46–50 artikla). Valvontaviranomaisen tehtävien suorittamisesta ei saa aiheutua kustannuksia rekisteröidylle eikä tietosuoja-vastaavalle. Jos pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia erityisesti siitä syystä, että niissä on toistuvuutta, valvontaviranomainen voi periä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimea. Valvontaviranomaisella on oltava tehokkaat tiedonsaanti- ja muut valtuudet (47 artikla).

Yhteistyö

Direktiivin 50 artiklaan on otettu säännökset jäsenvaltioiden valvontaviranomaisten velvollisuudesta tehdä keskinäistä yhteistyötä. Artiklassa säädetään muun muassa valvonta-asiassa tehtävässä yhteistyössä noudatettavasta menettelystä. Direktiivin 51 artiklassa puolestaan säädetään yleisellä tietosuoja-asetuksella perustetun tietosuojaneuvoston tehtävistä direktiivin soveltamisalalla. Neuvoston tehtäviin kuuluu antaa suosituksia direktiivin soveltamisesta sekä antaa komissiolle lausunto kolmannen maan tietosuojan tason riittävyydestä.

Oikeussuojakeinot, vastuu ja seuraamukset

Direktiivin 52 artiklassa säädetyn mukaisesti jokaisella rekisteröidyllä on oltava oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo häneen liittyvässä henkilötietojen käsittelyssä rikotun direktiivin nojalla annettuja säännöksiä. Valvontaviranomaisen on ilmoitettava rekisteröidylle valituksen etenemisestä ja ratkaisusta. Direktiivin 53 artiklassa säädetään, että luonnollisilla henkilöillä ja oikeushenkilöillä on oltava oikeus käyttää tehokkaita oikeussuojakeinoja valvontaviranomaisen oikeudellisesti sitovia heitä koskevia päätöksiä vastaan, sanotun kuitenkaan rajoittamatta muita hallinnollisia muutoksenhakekeinoja tai muita kuin oikeudellisia oikeussuojakeinoja. Jokaisella rekisteröidyllä on oltava oikeus tehokkaihin oikeussuojakeinoin, jos valvontaviranomainen ei ole käsitellyt valitusta tai ilmoittanut sen etenemisestä kolmen kuukauden kuluessa.

Jäsenvaltioiden on lisäksi 54 artiklan mukaisesti säädettävä, että rekisteröidyllä on oikeus tehokkaihin oikeussuojakeinoin, jos hän katsoo oikeuksiaan rikotun sen takia, ettei hänen henkilötietojensa käsittelyssä ole noudatettu lakia. Direktiivin 55 artiklassa säädetyn mukaisesti jäsenvaltioiden on kansallisen prosessioikeutensa mukaisesti säädettävä siitä, että rekisteröidyllä on oikeus valtuuttaa sellainen voitto tavoittelematon elin, järjestö tai yhdistys, jonka tavoitteet ovat yleisen edun mukaisia ja joka toimii henkilötietojen suojan edistämiseksi, tekemään valitus puolestaan ja käyttämään puolestaan 52, 53 ja 54 artiklassa tarkoitettuja oikeuksia.

Rekisteröidyllä on oltava oikeus saada korvausta aineettomasta tai aineellisesta vahingosta, joka tälle koituu direktiivin nojalla annettuja säännöksiä rikkovasta menettelystä (56 artikla). Jäsenvaltioiden on vahvistettava säännöt tämän direktiivin nojalla annettuihin säännöksiin kohdistuvien rikkomusten johdosta määrättävistä seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia (57 artikla).

Täytäntöönpanosäännökset ja loppusäännökset

Direktiivin 59 artiklassa säädetyn mukaisesti direktiivillä kumotaan neuvoston puitepäättös 2008/977/YOS. Direktiivin 63 artiklassa säädetyn mukaisesti jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään 6 päivänä toukokuuta 2018. Niiden on viipymättä ilmoitettava komissiolle kirjallisina nämä säännökset ja niitä on sovellettava 6 päivästä toukokuuta 2018. Jäsenvaltiot voivat kuitenkin säätää, että jos siitä aiheutuu suhteetonta vaivaa, voidaan ennen 6 toukokuuta 2016 luodut automatisoidut käsittelyjärjestelmät saattaa lokitietojen keräämistä koskevan 25 artiklan mukaisiksi viimeistään 6 toukokuuta 2023. Jos lokitietojen keräämistä koskevan veloitteen täyttämistä poikkeuksellisissa olosuhteissa aiheutuisi vakavia vaikeuksia automatisoidun käsittelyjär-

jestelmän toiminnalle, voidaan siirtymäaikaa pidentää enintään 6 toukokuuta 2026 asti.

Direktiivin 60 artiklan mukaan direktiivi ei vaikuta henkilötietojen suojaa koskeviin erityisiin säännöksiin, jotka sisältyvät ennen 6 päivää toukokuuta 2016 voimaan tulleisiin unionin säännöksiin.

Direktiivin 61 artiklassa säädetyn mukaan jäsenvaltioiden kolmansien maiden tai kansainvälisten järjestöjen kanssa tehdyt sopimukset, jotka ovat voimassa ennen direktiivin voimaantuloa ja joihin sisältyy henkilötietojen luovuttamista koskevia määräyksiä, säilyvät voimassa kunnes niitä muutetaan tai ne kumotaan, edellyttäen kuitenkin, että nämä sopimukset ovat ennen direktiivin hyväksymistä vallinneen EU-oikeuden mukaisia.

3 Nykytila

3.1 Suomen lainsäädäntö ja käytäntö

Perustuslain 10 §:n 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Viranomaisten rikosasioissa suorittamaa henkilötietojen käsittelyä koskevat yleislakeina henkilötietolaki (523/1999) ja viranomaisten toiminnan julkisuudesta annettu laki (621/1999, jäljempänä *julkisuuslaki*).

Suomessa henkilötietodirektiivi on pantu täytäntöön henkilötietolailla ja siihen myöhemmin tehdyillä muutoksilla sekä julkisuuslain 16 §:n 3 momentin säännöksillä. Henkilötietodirektiiviä täytäntöönpanevia säännöksiä sisältyy myös tietosuojalautakunnasta ja tietosuojavaltuutetusta annettuun lakiin (389/1994) ja asetukseen (432/1994) sekä rikoslain (39/1889) 38 luvun 1, 2 ja 8 (578/1995) ja 9 §:ään (525/1999) sekä 40 luvun 5 §:ään (604/2002).

Henkilötietolaki on yleislaki ja soveltamisalaltaan laajempi kuin henkilötietodirektiivi. Henkilötietolakia sovelletaan myös tietosuojapuitepäätöksen soveltamisalalla tapahtuvaan henkilötietojen käsittelyyn, jollei muualla laissa toisin säädetä.

Henkilötietojen käsittelyllä tarkoitetaan henkilötietolaissa kaikkia henkilötietoihin kohdistuvia toimenpiteitä, kuten esimerkiksi henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista ja tuhoamista. Henkilötietolakia sovelletaan sekä henkilötietojen automaattiseen käsittelyyn että muuhun käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Henkilötietolaissa on säännökset henkilötietojen käsittelyä koskevista yleisistä periaatteista, arkaluonteisten tietojen ja henkilötunnuksen käsittelemisestä, erityisiä tarkoituksia kuten tutkimusta varten tapahtuvasta henkilötietojen käsittelystä, henkilötietojen siirrosta kolmanteen maahan, tietoturvallisuudesta, henkilötietojen käsittelyn ohjauksesta ja valvonnasta sekä seuraamuksista.

Henkilörekisterin pitämiseen ja henkilötietojen käsittelyyn viranomaisissa sovelletaan lisäksi useita erityissäädöksiä.

Laissa oikeushallinnon valtakunnallisesta tietojärjestelmästä (372/2010) säädetään oikeushallinnon lainkäyttöasioiden käsittelyä ja täytäntöönpanoa palvelevasta oikeushallinnon valtakunnallisesta tietojärjestelmästä. Laissa säädetään tuomioistuimissa, syyttäjäviranomaisissa sekä oikeusapuviranomaisissa vireillä olevia ja ratkaistuja asi-

oita koskevien tietojen tallettamisesta, tietojen luovuttamisesta ja muusta käsittelystä. Tuomioistuimilla, syyttäväviranomaisilla ja oikeusaputoimistoilla on velvollisuus liittyä tietojärjestelmään ja toimittaa siihen tietoja. Oikeusrekisterikeskus on oikeushallinnon valtakunnallisen tietojärjestelmän rekisterinpitäjä. Tietojärjestelmään talletetut tiedot ovat salassa pidettäviä, eikä niitä siten voida luovuttaa, jollei laissa ole erikseen niin säädetty. Lain soveltamisalan ulkopuolelle jäävät viranomaiskohtaiset tietojärjestelmät.

Rikosrekisterilain (770/1993) mukaan rikosrekisteriin kerätään, talletetaan ja siitä luovutetaan tietoja, jotka tarvitaan rikosoikeudellisten seuraamusten määrittämistä ja täytäntöönpanoa varten. Oikeusrekisterikeskus on rikosrekisterin rekisterinpitäjä. Rikosrekisteriin talletetut tiedot ovat salassa pidettäviä eikä niitä voida luovuttaa, jollei laissa ole erikseen niin säädetty. Laissa säädetään myös tietojen poistamisesta rikosrekisteristä.

Laissa sakon täytäntöönpanosta (672/2002) säädetään sakkorekisterin pitämisestä. Oikeusrekisterikeskus on sakkorekisterin rekisterinpitäjä. Sakkorekisteriä pidetään ja käytetään sakon täytäntöönpanosta annetussa laissa säädettyssä järjestyksessä täytäntöön pantavien asioiden täytäntöönpanoa varten. Sakkorekisterin sisältämät rikokseen ja rikosoikeudelliseen seuraamukseen liittyvät tiedot on pidettävä salassa. Mainittuja tietoja saa luovuttaa vain niille, joiden oikeudesta tietojen saamiseen säädetään erikseen lailla. Laki sisältää myös säännökset tietojen poistamisesta sakkorekisteristä.

Laissa rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä (214/2012, jäljempänä *EU-rikosrekisterilaki*) säädetään rikosrekisterin ja sakkorekisterin tietojen toimittamisesta siihen EU:n jäsenvaltioon, jonka kansalainen tuomittu on sekä toisesta jäsenvaltiosta Suomeen toimitettujen Suomen kansalaista koskevien rekisteritietojen säilyttämisestä Suomessa. Rikosrekisterin ja sakkorekisterin tietoja luovutetaan tuomitun kansalaisuusjäsenvaltioon EU-rikosrekisterilain 5 §:n mukaisesti. Rikosrekisteritietojen luovuttamisesta toiseen pohjoismaahan säädetään lisäksi asetuksella.

Oikeusrekisterikeskus ylläpitää EU-rikosrekisterilain nojalla säilytysrekisteriä Suomeen toimitettujen Suomen kansalaista koskevien tietojen säilyttämistä varten niiden edelleen luovuttamiseksi toisiin jäsenvaltioihin ja Suomen viranomaisille sekä rikosrekisteriotteelle merkitsemiseksi. Säilytysrekisteriin merkityt tiedot on pidettävä salassa. EU-rikosrekisterilailla on pantu täytäntöön neuvoston puitepäättös jäsenvaltioiden välisen rikosrekisteritietojen vaihdon järjestämisestä ja sisällöstä (2009/315/YOS). Puitepäättöksessä vahvistetuilla säännöillä täydennetään poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamista koskevia olemassa olevia yleisiä sääntöjä. Puitepäättöksen mukainen tietojenvaihto

tapahtuu jäsenvaltioiden keskusviranomaisten välityksellä. Suomessa keskusviranomaisena toimii Oikeusrekisterikeskus.

Laissa henkilötietojen käsittelystä rikosseuraamuslaitoksessa (1069/2015) säädetään Rikosseuraamuslaitokselle kuuluvien rangaistusten täytäntöönpanotehtävien ja muiden tehtävien suorittamiseksi tarpeellisten henkilörekisterien pitämisestä ja muusta henkilötietojen käsittelystä. Laki koskee sakkorangaistusten täytäntöönpanoa vain sakon muuntorangaistuksen osalta. Ehdollisen vankeusrangaistuksen osalta laki koskee vain nuorille ehdollisen vankeuden tehosteeksi määrättyä valvontaa, koska ilman valvontaa tuomittu ehdollinen vankeusrangaistus ei edellytä täytäntöönpanotoimenpiteitä. Laki koskee myös Rikosseuraamuslaitoksen toteuttamaa tutkintavankeuden toimeenpanoa sekä Rikosseuraamuslaitoksen toimenpiteitä ja niissä tarvittavaa henkilötietojen käsittelyä seuraamukseen tuomitsemisen edellytyksiä selvittäessä tai seuraamuksen täytäntöönpanoa valmisteltaessa. Rikosseuraamuslaitoksen valtakunnallisia henkilörekistereitä ovat täytäntöönpanorekisteri, yhdyskuntaseuraamusrekisteri, valvonta- ja toimintarekisteri, turvallisuustietorekisteri ja tapaajarekisteri.

Ulosottokaareissa (705/2007) säädetään ulosoton tietojärjestelmästä, joka on ulosottoviranomaisille kuuluvien tehtävien hoitamista varten perustettu ja ulosottoviranomaisten valtakunnalliseen käyttöön tarkoitettu automaattisen tietojenkäsittelyn avulla ylläpidettävä tietojärjestelmä. Valtakunnanvoudinvirasto huolehtii tietojärjestelmän ylläpitämisestä ja kehittämisestä. Ulosoton tietojärjestelmään kuuluu ulosottorekisteri, joka koostuu valtakunnallisesta hakemisto-osasta ja paikallisesti ylläpidetyistä rekisterin osista. Ulosottorekisteriä pitävät paikalliset ulosottoviranomaiset yhdessä. Valtakunnanvoudinvirasto huolehtii rekisterin yleisestä ylläpidosta ja antaa määräyksiä tietojen teknisestä tallettamis- ja käsittelytavasta. Ulosottorekisteriä varten kerättyjen ja siihen talletettujen henkilötietojen käsittelyyn sovelletaan henkilötietolakia, jollei ulosottokaareissa toisin säädetä. Ulosottokaari sisältää säännökset muun muassa rekisteröidyn tarkastusoikeudesta, tietojen poistamisesta ulosottorekisteristä ja viranomaisten välisestä tietojen luovuttamisesta. Osa ulosottorekisteriin talletetuista tiedoista on salassa pidettäviä.

Rikosasioiden tietosuojadirektiivissä tarkoitettuja rikosasiaa koskevia tietoja luovutetaan toisista EU:n jäsenvaltioista Suomen viranomaisille yksittäiseen asiaan liittyen kansainvälistä rikosoikeudellista yhteistyötä koskevia säädöksiä sovellettaessa. Kansainvälinen rikosoikeudellinen yhteistyö kattaa muun muassa keskinäisen oikeusavun rikosasioissa, rikoksen johdosta tapahtuvan luovuttamisen sekä yhteistyön vankeusrangaistuksen ja muiden rikosoikeudellisten seuraamusten täytäntöönpanon siirtämiseksi.

Keskeisin kansainvälistä rikosoikeusapua koskeva säädös Euroopan unionin jäsenvaltioiden välillä on direktiivi 2014/41/EU rikosasioita koskevasta eurooppalaisesta

tutkintamääräyksestä. Suomessa direktiivi on pantu täytäntöön rikosasioita koskevaa eurooppalaista tutkintamääräystä koskevan direktiivin täytäntöönpanosta annetulla lailla (430/2017), joka tuli voimaan 3 päivänä heinäkuuta 2017.

Suhteessa niihin jäsenvaltioihin, joihin ei sovelleta tutkintamääräystä koskevaa direktiiviä, sovelletaan aikaisemmin voimassa ollutta sääntelyä. Tätä sääntelyä sovelletaan myös, kun kyse on sellaisesta rikosoikeusavusta, johon direktiiviä ei sovelleta. Keskeisimpiä tällaisia keskinäistä rikosoikeusapua koskevia monenvälisiä sopimuksia ovat Euroopan neuvoston keskinäistä oikeusapua rikosasioissa koskeva eurooppalainen yleissopimus (SopS 30/1981) ja keskinäisestä oikeusavusta rikosasioissa Euroopan unionin jäsenvaltioiden välillä vuonna 2000 tehty yleissopimus (SopS 56/2004). Kansainvälisestä oikeusavusta rikosasioissa säädetään lisäksi kansainvälisestä oikeusavusta rikosasioissa annetussa laissa (4/1994).

Euroopan unionin jäsenvaltioiden välinen rikoksen johdosta tapahtuva luovuttaminen perustuu eurooppalaisesta pidätysmääräyksestä tehtyyn puitepäätökseen (2002/584/YOS), joka on pantu Suomessa täytäntöön rikoksen johdosta tapahtuvasta luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä annetulla lailla (1286/2003). Rikoksen johdosta tapahtuvasta luovuttamisesta EU:n jäsenvaltioihin säädetään myös rikoksen johdosta tapahtuvasta luovuttamisesta Suomen ja muiden pohjoismaiden välillä annetussa laissa (1383/2007).

Tuomittujen siirto EU:n jäsenvaltioiden välillä perustuu puitepäätökseen (2008/909/YOS). Puitepäätös on pantu kansallisesti täytäntöön lailla tuomittujen siirtoa Euroopan unionissa koskevan puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta (1169/2011).

Sakkojen täytäntöönpanoa ja konfiskaatiopäätösten tunnustamista koskeva yhteistyö EU:ssa perustuu puitepäätöksiin 2005/214/YOS ja 2006/783/YOS, jotka on pantu täytäntöön vastavuoroisen tunnustamisen periaatteen soveltamisesta taloudellisiin seuraamuksiin tehdyn puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta annetulla lailla (231/2007) ja vastavuoroisen tunnustamisen periaatteen soveltamisesta menetetyksi tuomitsemista koskeviin päätöksiin tehdyn puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta annetulla lailla (222/2008).

Omaisuuksien jäädyttämistä koskeva yhteistyö perustuu puitepäätökseen 2003/577/YOS, joka on pantu kansallisesti täytäntöön lailla omaisuuden tai todistusaineiston jäädyttämistä koskevien päätösten täytäntöönpanosta Euroopan unionissa (540/2005).

EU:n jäsenvaltioiden välistä yhteistyötä sääntelee myös puitepäättös (2008/947/YOS), joka on pantu täytäntöön valvontatoimenpiteitä ja vaihtoehtoisia seuraamuksia Euroopan unionissa koskevan puitepäättöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäättöksen soveltamisesta annetulla lailla (1170/2011). Puitepäättös 2009/829/YOS on pantu kansallisesti täytäntöön lailla tutkintavankeuden vaihtoehtona määrättyjä valvontatoimia koskevan puitepäättöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäättöksen soveltamisesta (620/2012). Puitepäättös (2009/948/YOS) on pantu täytäntöön rikosoikeudellisia menettelyjä koskevien toimivaltaristiriitojen ehkäisemisestä ja ratkaisemisesta sekä esitutinnan ja syytetoimien siirtämisestä Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä annetulla lailla (295/2012). Eurooppalaisesta suojelumääräyksestä annettu direktiivi (2011/99/EU) on pantu täytäntöön eurooppalaisesta suojelumääräyksestä annetun Euroopan parlamentin ja neuvoston direktiivin lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja direktiivin soveltamisesta annetulla lailla (226/2015).

Rikosrekisteritietojen vaihtoa koskeva yhteistyö EU:n jäsenvaltioiden välillä perustuu puitepäättökseen (2009/315/YOS), joka on pantu täytäntöön rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä annetulla lailla (214/2012).

Henkilötietojen käsittelyä poliisitoimessa koskeva lainsäädäntö

Poliisin henkilötietojen käsittelyyn sovelletaan erityislakina lakia henkilötietojen käsittelystä poliisitoimessa (761/2003, poliisin henkilötietolaki). Poliisin henkilötietolaissa säädetään poliisiasiain tietojärjestelmästä, hallintoasiain tietojärjestelmästä, epäiltyjen tietojärjestelmästä ja Suojelupoliisin toiminnallisesta tietojärjestelmästä. Laissa säädetään myös muun muassa henkilötietojen käyttämisestä ja luovuttamisesta, poistamisesta ja arkistoinnista sekä kansainväliseen poliisiyhteistyöhön liittyvästä henkilötietojen käsittelystä. Edellä mainittujen tietojärjestelmien lisäksi useassa poliisia koskevassa erityislaissa säädetään poliisin yksittäisistä henkilörekistereistä, tai velvollisuudesta ylläpitää henkilötietoja sisältäviä tiedostoja. Tällaisia henkilörekistereitä ovat esimerkiksi rahanpesun selvittelykeskuksesta annetussa laissa (445/2017) tarkoitettu rahanpesurekisteri, todistajansuojeluohjelmasta annetussa laissa (88/2015) tarkoitettu todistajansuojelurekisteri, passilaissa (671/2006) tarkoitettu passirekisteri sekä ampu-ma-aselaissa (1/1998) tarkoitettut tiedostot lupa- ja valvontatehtävien suorittamiseksi. Lisäksi poliisin, tullin ja Rajavartiolaitoksen yhteistoiminnasta annetussa laissa (687/2009, jäljempänä *PTR-laki*) säädetään tietojen käsittelystä tilapäisessä rikosanalyysirekisterissä, jonka kukin näistä yhteistoimintaviranomaisista voi perustaa oman henkilötietojen käsittelyä koskevan lainsäädäntönsä nojalla. Poliisin henkilörekistereistä osa kuuluisi tietosuojasetuksen ja osa ehdotetun lain soveltamisalaan.

Poliisin henkilötietojen käsittelyä koskevia säännöksiä sisältyy myös eräisiin EU-säädöksiin ja niiden täytäntöönpanolakeihin, joita sovelletaan rikosasioiden tietosuojadirektiivin soveltamisalasäännöksessä tarkoitettuihin tehtäviin liittyvään EU:n jäsenvaltioiden väliseen poliisiyhteistyöhön. Näitä säännöksiä ovat erityisesti Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 1987/2006, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä tehty neuvoston päätös 2007/533/YOS sekä ajoneuvojen rekisteröintitodistusten myöntämisestä vastaavien jäsenvaltioiden yksiköiden pääsyn sallimisesta toisen sukupolven Schengenin tietojärjestelmään (SIS II) annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 1986/2006; Euroopan unionin lainvalvontayhteistyövirastosta annettu Euroopan parlamentin ja neuvoston asetus (EU) 2016/794 (Europol-asetus; ja laki Euroopan unionin lainvalvontayhteistyövirastosta, 214/2017); Euroopan parlamentin ja neuvoston asetus (EU) N:o 603/2013 Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013 tehokkaaksi soveltamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä (Eurodac-asetus); rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajat ylittävän rikollisuuden torjumiseksi tehty neuvoston päätös 2008/615/YOS ja sen täytäntöönpanopäätös 2008/616/YOS; sekä tietojen ja tiedustelutietojen luovuttamisesta Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta tehty neuvoston puitepätös 2006/960/YOS (ja Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta tehdyn puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta annettu laki (26/2009).

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/681 matkustajarekisteritietojen (*Passenger Name Record*, PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syyte-toimia varten (jäljempänä *matkustajatietodirektiivi*) annettiin 27 päivänä huhtikuuta 2016, ja sen täytäntöönpano on vielä kesken. Matkustajatietodirektiivin täytäntöönpanosäännöksistä osa koskisi henkilötietojen käsittelyä, johon ehdotettua lakia sovellettaisiin täydentävin osin.

Henkilötietojen käsittelyä Puolustusvoimissa koskeva lainsäädäntö

Puolustushallinnossa ei ole tällä hetkellä keskitettyä lainsäädäntöä henkilötietojen käsittelystä, vaan säännökset on hajautettu useisiin eri lakeihin. Erityissääntelyä on

asevelvollisuuslaissa (1438/2007), puolustusvoimista annetussa laissa (551/2007), sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa (255/2014), aluevalvontalaissa (755/2000) ja sotilaallisesta kriisinhallinnasta annetussa laissa (211/2006). Lisäksi vapaaehtoisesta maanpuolustuksesta annetussa laissa (556/2007) on säännöksiä Maanpuolustuskoulutusyhdistyksen suorittamasta henkilötietojen käsittelystä. Säännökset koskevat lähinnä Puolustusvoimien pysyviä henkilörekistereitä, niihin talletettavia tietoja, tiedonsaanti- ja luovutusoikeuksia sekä tiettyjä rekisteröidyn oikeuksien rekisterikohtaisia rajoituksia. Muilta osin Puolustusvoimien suorittamaan henkilötietojen käsittelyyn sovelletaan yleisen henkilötietolain säännöksiä.

Henkilötietojen käsittelyä Tullissa koskeva lainsäädäntö

Laissa henkilötietojen käsittelystä Tullissa (639/2015, myöhemmin *Tullin henkilötietolaki*) säädetään Tullin henkilörekistereistä ja henkilötietojen käsittelystä. Tullin pysyviä henkilörekistereitä ovat rikostorjunnan tietojärjestelmä, tiedustelurekisteri, tullivalvonnan tietojärjestelmä ja rekisterikilpien ja konttien kuvaus- ja tunnistusjärjestelmä.

Lain soveltamisala kattaa Tullille laissa säädettyjen tehtävien suorittamiseksi tarpeellisten henkilötietojen automaattisen käsittelyn ja muun henkilötietojen käsittelyn, jos ne muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Tullin henkilötietolain lähtökohtana on, että voimassa olevasta henkilötietolaista ja viranomaisten toiminnan julkisuudesta annetusta laista poiketaan vain, jos se on tullitoiminnan tehokkuuden turvaamiseksi tai Euroopan unionin tulli- tai muita tietojärjestelmiä koskevien määräysten huomioon ottamiseksi välttämätöntä. Sanotuista laeista poiketaan laissa lähinnä arkaluonteisten tietojen keräämistä ja tallettamista, rekisteröidyn tarkastusoikeutta sekä henkilötietojen käyttöä ja luovuttamista koskevien säännösten osalta. Laissa säädetään lisäksi myös henkilörekisterin perustamisesta, Tullin henkilörekisterien tietosisällöstä, tietojen käsittelystä, rekisterin pitäjästä, henkilörekisterien tietojen säilytysajoista, kansallisesta ja kansainvälisestä tietojenvaihdosta sekä rekisterien käytön valvonnasta. Rikostorjuntaan liittyvän viranomaisyhteistyön ja tiedonvaihdon tehostamiseksi Tullin henkilötietolaki on säädetty mahdollisemman pitkälle yhdenmukaiseksi henkilötietojen käsittelystä poliisitoimessa annetun lain kanssa. Merkittävimmät erot johtuvat näiden viranomaisten erilaisista tehtävistä, käytössä olevista tietojärjestelmistä ja rekistereistä. Tullin henkilörekistereistä osa kuuluisi tietosuoja-asetuksen ja osa ehdotetun lain soveltamisalaan. Tullissa sovelletaan lisäksi eräitä edellä mainittuja poliisinkin toimintaan sovellettavia EU-säädöksiä ja niiden täytäntöönpanolakeja lainvalvontaviranomaisten välisestä yhteistyöstä rikosasioiden tietosuojadirektiivin soveltamisalalla.

Henkilötietojen käsittelyä Rajavartiolaitoksessa koskeva lainsäädäntö

Rajavartiolaitoksen henkilötietojen käsittelyyn sovelletaan erityislakina henkilötietojen käsittelystä rajavartiolaitoksessa annettua lakia (579/2005, *Rajavartiolaitoksen henkilötietolaki*). Rajavartiolaitoksen henkilötietolaissa säädetään Rajavartiolaitoksen pysyvistä valtakunnallisista henkilörekistereistä, joita ovat tutkinta- ja virka-apurekisteri, lupa-asioiden rekisteri, valvonta-asioiden rekisteri, rikoksesta epäiltyjen Rajavartiolaitoksen rekisteri, turvallisuustietorekisteri, sotilasoikeudenhoidon rekisteri ja kurinpitoratkaisurekisteri. Laissa säädetään myös muiden valtakunnallisten tai alueellisten henkilörekisterien perustamisesta, henkilötietojen käyttämisestä ja luovuttamisesta, poistamisesta ja arkistoinnista sekä kansainväliseen yhteistyöhön liittyvästä henkilötietojen käsittelystä. Henkilötietojen käsittelystä meripelastustoimessa ja meripelastusrekisteristä säädetään meripelastuslaissa (1145/2001) ja asevelvollisrekisteristä asevelvollisuuslaissa (1438/2007). Rajavartiolaitoksessa sovelletaan lisäksi eräitä edellä mainittuja poliisinkin toimintaan sovellettavia EU-säädöksiä ja niiden täytäntöönpanolakeja lainvalvontaviranomaisten välisestä yhteistyöstä rikosasioiden tietosuojadirektiivin soveltamisalalla.

3.2 Kansainväliset velvoitteet

3.2.1 EU:n lainsäädäntö

Euroopan unionin perusoikeuskirjan 8 artiklan 1 kohdan ja Euroopan unionin toiminnasta tehdyn sopimuksen (jäljempänä *SEUT*) 16 artiklan 1 kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan. Perusoikeuskirjan 8 artiklan mukaan henkilötietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.

Vuonna 1995 laaditun henkilötietodirektiivin tarkoituksena oli yhdenmukaistaa luonnollisten henkilöiden henkilötietojen käsittelyä koskevien perusoikeuksien ja -vapauksien suojelua ja taata henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä. Henkilötietodirektiiviä sovelletaan osittain tai kokonaan automatisoituun tietojenkäsittelyyn sekä sellaisten henkilötietojen manuaaliseen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Henkilötietodirektiiviä ei sovelleta rikosasioissa tehtävään poliisi- ja oikeudelliseen yhteistyöhön.

EU:n tietosuojapuitepäättös 2008/977/YOS koskee EU:n jäsenvaltioiden rajat ylittävää henkilötietojen käsittelyä rikosasioissa. Ennen tietosuojapuitepäättöksen hyväksymistä EU:ssa ei ollut rikosasioissa tehtävää poliisi- ja oikeudellista yhteistyötä koskevia yhtenäisiä tietosuojasäännöksiä, joskin erityissääntelyä on sisältynyt esimerkiksi vuoden 2002 Eurojust-päätökseen. Tietosuojapuitepäättös eroaa rikosasioiden tietosuojadirektiivistä muun muassa soveltamisalansa osalta, sillä se koskee vain henkilötietojen vaihtoa jäsenvaltioiden toimivaltaisten viranomaisten kesken. Puitepäättös myös sisältää rikosasioiden tietosuojadirektiiviä enemmän kansallista liikkumavaraa.

3.2.2 Kansainväliset sopimukset

Henkilötietojen suoja on käsitteellisesti läheisesti kytköksissä yksityiselämän suojaan. Yksityiselämän suoja on keskeinen useissa kansainvälisissä ihmisoikeussopimuksissa turvattu oikeus. Oikeutta yksityiselämän suojaan koskevat muun muassa Euroopan ihmisoikeussopimuksen (SopS 19/1990) 8 artikla, kansalais- ja poliittisia oikeuksia (SopS 7–8/1976) koskevan kansainvälisen yleissopimuksen 17 artikla sekä lapsen oikeuksien yleissopimuksen (SopS 59–60/1991) 16 artikla.

Henkilötietojen suojaa koskevaan lainsäädäntöön Euroopassa on merkittäväällä tavalla vaikuttanut Euroopan neuvoston piirissä laadittu yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä koskeva yleissopimus (SopS 35–36/1992, jäljempänä *tietosuojayleissopimus*). Euroopan neuvosto hyväksyi tietosuojayleissopimuksen vuonna 1981, ja se on toiminut pohjana myös henkilötietodirektiiville.

Yleissopimus oli ensimmäinen oikeudellisesti sitova kansainvälinen instrumentti tietosuojan alalla. Yleissopimuksen määräykset tarjoavat minimisuojan henkilötietojen käsittelyssä kaikille sen ratifioineiden valtioiden alueilla oleskeleville henkilöille sekä rajat ylittävissä henkilötietojen siirroissa. Se velvoittaa sopimuspuolet sisällyttämään kansalliseen lainsäädäntöönsä toimenpiteet, joilla varmistetaan, että yksilöiden oikeuksia kunnioitetaan henkilötietoja käsiteltäessä. Tietosuojayleissopimusta sovelletaan automaattiseen henkilötietojen käsittelyyn, ja se koskee kaikkea henkilötietojen käsittelyä, mukaan lukien henkilötietojen käsittelyä poliisi- ja rikosoikeudellisen yhteistyön alalla. Yleissopimuksen nojalla on annettu myös lukuisia henkilötietojen käsittelyä koskevia suosituksia.

Sopimuksen on ratifioinut 47 Euroopan neuvoston jäsenvaltiota ja kolme Euroopan neuvoston ulkopuolista valtiota. Kaikki EU:n jäsenvaltiot ovat yleissopimuksen sopimuspuolia. Suomen osalta sopimus tuli voimaan vuonna 1992. Tietosuojayleissopimusta täydennettiin vuonna 2001 valvontaviranomaisia ja tietojen siirtoa rajojen yli koskevalla lisäpöytäkirjalla (ETS nro 181). Lisäpöytäkirjan on ratifioinut 36 Euroopan neuvoston jäsenvaltiota, mukaan lukien Suomi. Lisäksi lisäpöytäkirjan on ratifioinut

kolme Euroopan neuvoston ulkopuolista valtiota. Lisäpöytäkirja tuli Suomen osalta voimaan vuonna 2012.

Euroopan neuvostossa on laadittu lisäpöytäkirjaluonnos yleissopimuksen mukauttamiseksi nykyisiin ja tuleviin tietosuojahaasteisiin. Neuvottelut asiasta jatkuvat.

3.2.3 Ulkomaiden lainsäädäntö

Rikosasian käsittelyn yhteydessä sovellettava henkilötietolainsäädäntö on EU-maissa nykyisellään verraten epäyhtenäistä. Tämä johtuu muun muassa siitä, että henkilötiedirektiivi ei koske tällaista käsittelyä. Myöskään tietosuojapuitepäättöksen täytäntöönpano ei ole johtanut jäsenmaiden kansallisen lainsäädännön merkittävään lähentymiseen puitepäättöksen soveltamisalan rajauksista sekä sen jäsenvaltioille jättämästä liikkumavarasta johtuen.

Koska EU:n jäsenmaiden lainsäädäntö on rikosasioiden tietosuojadirektiivin kansallisen täytäntöönpanon vuoksi parhaillaan merkittävästi muuttumassa, ja koska direktiivi asettaa varsin kattavia ja yksityiskohtaisia vaatimuksia kansalliselle lainsäädännölle, ei tässä esityksessä ole tarkoituksenmukaista tarkemmin kuvata muiden maiden voimassa olevaa lainsäädäntöä. EU-maiden nykyistä lainsäädäntöä tarkastellaan vaikutustenarviointiasiakirjassa, jonka komissio julkaisi yhdessä direktiiviehdotuksen kanssa (SEC(2012) 72 final).

3.2.4 Kolmansien valtioiden kanssa tehdyt sopimukset

Rikosasioiden tietosuojadirektiivin 61 artiklan mukaan henkilötietojen siirtoa kolmansiin maihin tai kansainvälisille järjestöille edellyttävät kansainväliset sopimukset, joita jäsenvaltiot ovat tehneet ennen 6 päivää toukokuuta 2016 ja jotka ovat unionissa kyseisenä päivänä voimassa olleen oikeuden mukaisia, ovat edelleen voimassa, kunnes niitä muutetaan tai ne korvataan tai kumotaan.

4 Nykytilan arviointi

Rikosasioiden tietosuojadirektiivin täytäntöönpano kansallisella tasolla edellyttää uuden lainsäädännön antamista. Ottaen huomioon, että henkilötietolaki on tarkoitus kumota, ja että yhtäältä yleinen tietosuoja-asetus sekä ehdotettu sitä täydentävä kansallinen laki ja toisaalta tietosuojadirektiivi ja sen täytäntöönpaneva lainsäädäntö muodostavat yhteisistä peruseriaateistaan huolimatta toisistaan selvästi erilliset kokonaisuudet, ehdotetaan tässä esityksessä erillisen rikosasioiden käsittelyssä noudatettavaksi tulevan henkilötietolain säätämistä. Koska lakia soveltavilla viranomaisilla, erityisesti poliisilla, Rajavartiolaitoksella, puolustusvoimilla ja tullilla on erilaisia tehtäviä ja toimivaltuuksia, on lainsäädäntöä tarpeen täydentää hallinnonalakohtaisella erityissääntelyllä.

Eräiltä osin direktiivin säännökset eivät edellytä uutta kansallista sääntelyä. Tällaisia direktiivin säännöksiä ovat esimerkiksi eräät valvontaviranomaisen menettelyä koskevat säännökset, joiden osalta ei ole tarpeen ottaa lainsäädäntöön uusia säännöksiä, koska näistä asioista säädetään Suomessa sovellettaviksi tulevissa hallinnon yleislajeissa. Esimerkiksi direktiivin 52 artiklan 2 kohdassa edellytetyn mukaisesti jäsenvaltioiden on säädettävä siitä, että sellaisen valvontaviranomaisen, joka ei ole asiassa toimivaltainen, on toimitettava sille tehty valitus toimivaltaiselle viranomaiselle. Asiasta ei ole tarpeen säätää tässä yhteydessä, sillä asiakirjan siirtämisestä toimivaltaiselle viranomaiselle säädetään hallintolain (434/2003) 21 §:ssä.

Lisäksi direktiivissä on säännöksiä esimerkiksi yleisellä tietosuoja-asetuksella perustetun tietosuojaneuvoston tehtävistä direktiivin soveltamisalalla (51 artikla), komiteamenettelystä (58 artikla) ja komission kertomuksista (62 artikla), joita ei ole tarpeen saattaa osaksi kansallista lainsäädäntöä.

5 Tavoitteet ja keskeiset ehdotukset

5.1 Tavoitteet

Esityksen tavoitteena on panna täytäntöön EU:n rikosasioiden tietosuojadirektiivi Suomessa. Direktiivi velvoittaa saavutettavaan tulokseen nähden jokaista jäsenvaltiota, jolle se on osoitettu, mutta jättää kansallisten viranomaisten valittavaksi muodon ja keinot. Vaikka rikosasioiden tietosuojadirektiivi edellyttää kansallisen lainsäädännön antamista direktiivin täytäntöönpanemiseksi, jättää se kuitenkin eräiltä osin jäsenvaltioille harkinnanvaraa erityisesti sääntelyn yksityiskohtien osalta.

Rikosasioiden tietosuojadirektiivissä todetaan, ettei sen kansallinen täytäntöönpano saisi johtaa henkilötietojen suojan tason heikentymiseen. Direktiivi ei myöskään estä jäsenvaltioita säätämästä direktiivissä edellytettyä korkeammasta rekisteröidyn oikeuksien suojan tasosta. Tässä esityksessä on otettu huomioon voimassa olevan henkilötietolain sääntely, ja eräiltä osin pyritty turvaamaan rekisteröidyn oikeuksia direktiivin edellyttämää vähimmäistasoa paremmin. Ehdotettuun täytäntöönpanolakiin on esimerkiksi otettu säännökset henkilötunnuksen käsittelemisestä, vaikka sitä koskevia säännöksiä ei rikosasioiden tietosuojadirektiivissä olekaan.

Esityksen laadinnassa on pääministeri Sipilän hallitusohjelman EU-lainsäädännön täytäntöönpanoa koskevan kirjauksen mukaisesti pyritty välttämään kansallista lisäsääntelyä.

Kaikki rikosasioiden tietosuojadirektiiviä toimeenpanevaa lainsäädäntöä soveltavat viranomaiset soveltavat toiminnassaan myös yleistä tietosuoja-asetusta. Tästä syystä ehdotettua lainsäädäntöä valmisteltaessa on lainsäädännön yhtenäisyyden edistämiseksi pyritty seuraamaan asetuksessa ja hallituksen esityksessä sitä täydentäväksi lainsäädännöksi käytettyjä sisällöllisiä ja terminologisia ratkaisuja siltä osin, kuin ei ole ollut painavia syitä päätyä toisenlaiseen ratkaisuun.

5.2 Keskeiset ehdotukset

Ehdotetun lain soveltamisala

Ehdotettu laki on luonteeltaan rikosasioiden käsittelyssä tietosuojan osalta yleislakina noudatettava laki. Se olisi toissijainen muuhun lainsäädäntöön nähden. Jos muussa

laissa on ehdotetusta laista poikkeavia säännöksiä, on niitä noudatettava ehdotetun lain sijasta. Lakia soveltavien toimivaltaisten viranomaisten erilaiset tehtävät ja valtuudet huomioon ottaen sektorikohtaiselle sääntelylle voidaan Suomessa katsoa olevan tarvetta, ja tällaista lainsäädäntöä onkin valmisteltu samanaikaisesti tämän esityksen kanssa. On selvää, että sovellettavan lainsäädännön on kokonaisuudessaan oltava sopusoinnussa rikosasioiden tietosuojadirektiivin ja Suomea velvoittavien kansainvälisten sopimusten kanssa.

Lain sovellettavaksi tulemisen kannalta on tarpeen ottaa huomioon sekä sen aineellinen että organisatorinen soveltamisala. Lakia soveltaisivat viranomaiset, joiden toimivalta kattaa rikosten ennalta estämisen, tutkimisen, paljastamisen tai rikoksiin liittyvät syytetoimet, rikosoikeudellisiin seuraamuksiin tuomitsemisen tai niiden täytäntöönpanon. Tällaisia viranomaisia ovat muun muassa poliisi, Rajavartiolaitos, Tulli, syyttäjät, tuomioistuimet ja Rikosseuraamuslaitos. Nämä viranomaiset soveltaisivat ehdotettua lakia kuitenkin vain, kun ne käsittelevät henkilötietoja edellä mainitussa tarkoituksessa, eli esimerkiksi rikoksen selvittämisen yhteydessä tai käsiteltäessä rikosasiaa tuomioistuimessa. Esimerkiksi poliisin käsitellessä henkilötietoja hakemusasian yhteydessä tulisi sovellettavaksi ehdotetun lain sijasta yleinen tietosuoja-asetus ja sitä täydentävä kansallinen lainsäädäntö.

Lakia sovellettaisiin lisäksi toimivaltaisten viranomaisten kansallisen turvallisuuden ylläpitämisen yhteydessä tapahtuvaan henkilötietojen käsittelemiseen. Toimivaltaisista viranomaisista ovat tältä osin puolustusvoimat, Rajavartiolaitos ja poliisi, erityisesti suojelupoliisi. Tältä osin ehdotetun lain soveltamisala ei perustu direktiivin toimeenpanoon, vaan kysymys on kansallisesta ratkaisusta. Kansallisen turvallisuuden ylläpitäminen jää nimenomaisten säännösten perusteella sekä yleisen tietosuoja-asetuksen että rikosasioiden tietosuojadirektiivin soveltamisalan ulkopuolelle. Jotta henkilötietojen käsittelyä koskevaan lainsäädäntöön ei kansallisen turvallisuuden ylläpitämiseen tähtäävän toiminnan yhteydessä jää katvealuetta ja perustuslain 10 §:n 1 momentin lailla säättämisen vaatimus tulee täytettyä, on näihin tilanteisiin sovellettavasta lainsäädännöstä säädettävä kansallisella tasolla. Rikosasioiden tietosuojadirektiivin täytäntöönpanolaissa on yleiseen tietosuoja-asetukseen verrattuna sääntelyn kohteesta johtuen jossakin määrin painotettu enemmän viranomaisen tarvetta eräissä tilanteissa rajoittaa rekisteröidyn oikeuksia, kuten esimerkiksi rekisteröidyn tarkastusoikeutta. Ottaen huomioon, että kansallisen turvallisuuden alalla on vastaavia viranomaistarpeita, on kansallisen turvallisuuden ylläpitämisen yhteydessä tapahtuva henkilötietojen käsittely tarkoituksenmukaista sisällyttää tässä esityksessä ehdotettavaan direktiivin täytäntöönpanolakiin siltä osin kuin erityislainsäädännössä ei toisin säädettäisi.

Henkilötietojen käsittelyn yleiset edellytykset

Ehdotettuun 2 lukuun otettaisiin säännökset henkilötietojen käsittelyn yleisistä edellytyksistä lain soveltamisalalla. Ehdotetun lain soveltamisalalla tapahtuvan henkilötietojen käsittelemisen tulee aina perustua lakiin ja sen tulee olla tarpeen toimivaltaisen viranomaisen ehdotetussa laissa tarkoitettujen tehtävien hoitamiseksi. Rekisterinpitäjä saa kuitenkin käsitellä henkilötietoja myös arkistointia taikka tieteellistä, tilastollista tai historiallista käsittelyä varten. Käsiteltävien henkilötietojen tulee olla virheettömiä sekä käsittelyn tarkoituksen kannalta asianmukaisia, päivitettyjä ja tarpeellisia. Sellaiset henkilötiedot, jotka koskevat eri asemassa olevia henkilöitä, kuten asianomistajia, todistajia tai epäiltyjä, tulee tarvittaessa ja mahdollisuuksien mukaan erottaa toisistaan.

Kun henkilötietoja siirretään EU:ssa sijaitsevalle vastaanottajalle, tietoja siirtävä viranomainen ei saa asettaa tietojen käsittelylle tiukempia edellytyksiä kuin mitä sovelletaan samankaltaisiin tiedonsiirtoihin kansallisesti. Tietoja siirtävän viranomaisen on informoitava vastaanottajaa velvollisuudesta noudattaa mahdollisia tietojen käyttämistä koskevia lakisääteisiä rajoituksia.

Ehdotettuun lakiin otettaisiin erityisiä henkilötietoryhmiä koskevia säännöksiä. Erityisiin henkilötietoryhmiin kuuluvia tietoja, joita ehdotetussa laissa kutsuttaisiin myös arkaluonteisiksi tiedoiksi, ovat henkilötiedot, joista ilmenee etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus taikka ammattiliiton jäsenyys, sekä geneettiset tiedot, luonnollisen henkilön yksiselitteiseen tunnistamiseen tarkoitetut biometriset tiedot tai terveyttä taikka luonnollisen henkilön seksuaalista käyttäytymistä ja seksuaalista suuntautumista koskevat tiedot. Tällaisten tietojen käsittely on sallittua vain, jos se on välttämätöntä ja edellyttäen, että rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu.

Lakiin otettaisiin myös säännökset, joilla rajoitetaan henkilötunnuksen käsittelemistä sekä merkitsemistä asiakirjoihin. Ehdotus ei tältä osin perustu rikosasoiden henkilötietodirektiiviin, vaan kyseessä on kansallinen ratkaisu. Ehdotettu sääntely vastaa olennaisilta osiltaan henkilötietolain sääntelyä.

Lakiin otettaisiin säännökset automatisoiduista yksittäispäätöksistä. Rikosasoiden tietosuojadirektiivi edellyttää, että päätös, joka perustuu pelkästään automatisoituun käsittelyyn, kuten profilointiin, ja jolla on rekisteröityä koskevia kielteisiä oikeusvaikutuksia tai joka vaikuttaa häneen merkittävästi, on kielletty, jollei sitä ole sallittu rekisterinpitäjään sovellettavassa unionin oikeudessa tai tietyt edellytykset täyttävässä jäsenvaltion lainsäädännössä. Rekisteröidyllä tulee olla oikeus vaatia, että luonnollinen henkilö osallistuu päätöksentekoon rekisterinpitäjän puolesta. Suomessa esimerkiksi poliisi ei tee edellä kuvatun kaltaisia automatisoituja yksittäispäätöksiä. Esityksessä

ehdotetaankin säädettäväksi kielto tehdä mainittuja päätöksiä. Kielto ei kuitenkaan estäisi säätämästä muualla laissa tällaisten päätösten tekemisestä, jolloin kyseisen lainsäädännön on oltava sopusoinnussa direktiivin vaatimusten kanssa.

Rekisterinpitäjän ja henkilötietojen käsittelijän vastuu

Rekisterinpitäjä vastaisi ehdotetun yleislain mukaan henkilötietojen käsittelyn lainmukaisuudesta. Sen tulisi toteuttaa käsittelyn lainmukaisuuden varmistamiseksi tarvittavat tekniset ja organisatoriset toimenpiteet. Lakiin otettaisiin myös säännökset oletusarvoisesta ja sisäänrakennetusta tietosuojasta sekä säännökset vastuunjaosta tilanteissa, joissa kaksi tai useampi rekisterinpitäjä yhdessä määrittävät käsittelyn tarkoitukset ja keinot. Ehdotettu sääntely perustuu direktiivin lainsäädäntötoimeksiantoon.

Henkilötietojen käsittelijän, eli henkilötietoja rekisterinpitäjän lukuun käsittelevän, on ehdotetun lain mukaan annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä muutoinkin riittävät takeet niistä organisatorisista ja teknisistä toimituksista, joilla se varmistaa, että henkilötietoja käsitellään laissa säädettyjen vaatimusten mukaisesti. Henkilötietojen käsittelijän suorittamasta käsittelystä on tehtävä kirjallinen sopimus, josta ilmenevät muun muassa käsittelyn luonne, tarkoitus ja kesto. Näistä seikoista voidaan määrätä myös muulla henkilötietojen käsittelijää sitovalla oikeustoimella. Ehdotukset perustuvat tältäkin osin direktiiviin.

Rekisterinpitäjän ja henkilötietojen käsittelijän olisi ehdotetun lain mukaan säilytettävä lokitiedot automaattisessa tietojenkäsittelyjärjestelmässään suoritetusta henkilötietojen keräämisestä, muuttamisesta, kyselystä, luovuttamisesta, siirtämisestä, yhdistämisestä ja poistamisesta. Lakiin otettaisiin myös säännökset velvollisuudesta tehdä tietosuojaa koskeva vaikutustenarviointi ennen henkilötietojen käsittelyn aloittamista. Eräissä tilanteissa vaikutustenarviointi olisi tehtävä kirjallisesti. Jos vaikutustenarviointi osoittaa, että rekisterinpitäjän suunnittelemista suojatoimenpiteistä huolimatta käsittely saattaa aiheuttaa merkittävän riskin rekisteröidyn oikeuksille, olisi rekisterinpitäjän tai henkilötietojen käsittelijän kuultava Tietosuojavirastoa. Jos virasto katsoo, että käsittely muodostuisi lainvastaiseksi, sen on pääsäännön mukaan kuuden viikon kuluessa annettava rekisterinpitäjälle tai henkilötietojen käsittelijälle ohjausta käsittelyn saattamiseksi lainmukaiseksi. Myös tältä osin ehdotuksessa on kyse direktiivin täytäntöönpanosta.

Rekisteröidyn oikeudet

Yleislaissa ehdotetaan säädettävän rekisterinpitäjälle velvollisuus ylläpitää yleisesti saataville asetettavaa tietosuojaselostetta. Selosteesta tulisi ilmetä muun muassa henkilötietojen käsittelyn tarkoitukset ja oikeusperuste, henkilötietojen mahdollinen

säilytysaika, henkilötietojen säännönmukaiset vastaanottajat sekä rekisterinpitäjän ja tietosuojavastaavan yhteystiedot. Sääntely perustuisi osittain direktiiviin ja osittain henkilötietolain sääntelyyn, edellyttäen direktiivissä säädettyä laajemmin julkisen selosteen laatimista. Rikosasioiden tietosuojadirektiivissä edellytetään siinä tarkoitettujen tietojen asettamista rekisteröidyn saataville, kun taas ehdotetussa yleislaissa edellytettäisiin selkeämmin selosteen julkistamista.

Yleislaissa säädettäisiin rekisteröidyn tarkastusoikeudesta eli oikeudesta saada tieto siitä, käsitelläänkö häntä koskevia tietoja sekä oikeus saada tällaiset tiedot samoin kuin tieto käsittelyn tarkoituksista. Rekisteröidyllä olisi niin ikään oikeus saada häntä koskevat, käsittelyn kannalta puutteelliset tai virheelliset henkilötiedot täydennettyä tai oikaistua. Rekisteröidyn näitä oikeuksia voidaan kuitenkin rajoittaa, jos se rekisteröidyn oikeudet huomioon ottaen on oikeasuhtaista ja välttämätöntä, jotta vältetään tuottamasta haittaa rikosten ennalta estämiselle, paljastamiselle, selvittämiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle, tai jos rajoittaminen on oikeasuhtaista ja välttämätöntä muun muassa kansallisen turvallisuuden suojelemiseksi. Rekisteröidyllä on oikeus pyytää Tietosuojavirastoa toimimaan puolestaan asiassa, jos rekisterinpitäjä rajoittaa hänen oikeuksiaan edellä mainitulla perusteella. Tietosuojaviraston on kohtuullisen ajan kuluessa ilmoitettava rekisteröidylle toimenpiteistä, joihin se on ryhtynyt. Ehdotettu sääntely perustuu tältä osin direktiiviin.

Direktiivin 12 artiklan 4 kohta edellyttää, että rekisteröidyn oikeuksien käyttö on tälle maksutonta. Jos rekisteröidyn pyynnöt ovat esimerkiksi niiden toistuvuudesta johtuen ilmeisen perusteettomia tai kohtuuttomia, rekisterinpitäjä voisi kuitenkin periä kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimea. Ehdotetussa yleislaissa säädettäisiin rekisteröidyn oikeuksien käyttämisen maksuttomuudesta. Laissa säädettäisiin rekisterinpitäjän mahdollisuudesta periä valtion maksuperustelain mukainen maksu, jos rekisteröidyn pyyntö on ilmeisen perusteeton tai kohtuuton. Esityksessä ei ehdoteta, että rekisterinpitäjä voisi tällaisessa tilanteessa kieltäytyä kokonaan rekisteröidyn pyynnön toteuttamisesta, koska tarkastusoikeudella sekä oikeudella saada tiedot täydennettyä tai oikaistua voi olla huomattavaa merkitystä rekisteröidyn oikeuksien toteutumisen kannalta ja koska maksun perimismahdollisuuden voidaan arvioida riittävästi ehkäisevän esimerkiksi toistuvien perusteettomien pyyntöjen tekemistä.

Tietoturvallisuus

Ehdotetussa yleislaissa säädetään direktiivin lainsäädäntötoimeksiannon mukaisesti rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudesta teknisin ja organisatorisin toimenpitein suojata henkilötiedot sellaisella tavalla, joka vastaa käsittelystä rekisteröityjen oikeuksille aiheutuvaa riskiä. Henkilötietojen käsittelijän tulisi tietoturvaloukkauksesta tiedon saatuaan ilman aiheutonta viivytystä ilmoittaa loukkauksesta rekiste-

rinpitäjälle. Rekisterinpitäjän puolestaan on ilmoitettava loukkauksesta Tietosuojavirastolle, paitsi jos loukkauksesta ei todennäköisesti aiheudu vaaraa rekisteröidyn oikeuksille. Yleislakiin otettaisiin myös säännökset rekisterinpitäjän velvollisuudesta ilmoittaa tietoturvaloukkauksesta rekisteröidyille, eräin laissa luetelluin poikkeuksin.

Rekisterinpitäjän tulisi ehdotetun yleislain mukaan ilmoittaa tietoturvaloukkauksesta myös sellaiselle Suomessa tai toisessa EU:n jäsenmaassa sijaitsevalle rekisterinpitäjälle, jonka toimittamiin tai jolle toimitettuihin tietoihin loukkaus kohdistuu. Direktiivi edellyttää säädettävän ainoastaan toisen EU-maan rekisterinpitäjälle tehtävästä ilmoituksesta, mutta yhtä lailla toisella Suomessa sijaitsevalla rekisterinpitäjällä on tarve saada tietää mainitunlaisesta tietoturvaloukkauksesta.

Henkilötietojen siirrot kolmansiin maihin

Yleislakiin otettaisiin direktiivin edellyttämät säännökset niistä yleisistä edellytyksistä, joiden vallitessa toimivaltainen viranomainen saa siirtää henkilötietoja kolmanteen maahan. Siirron olisi ensinnäkin oltava tarpeen ehdotetun lain soveltamisalasäännöksessä lueteltuja tarkoituksia varten, esimerkiksi rikoksen selvittämiseksi tai rangaistuksen täytäntöönpanemiseksi. Komission olisi lisäksi tullut todeta kyseisen maan tietosuojan tason olevan riittävä. Siirto kolmanteen maahan on eräin tarkoin säädeltävin edellytyksin mahdollista myös tilanteessa, jossa komissio ei ole tehnyt kyseistä maata koskevaa päätöstä tietosuojan riittävästä tasosta.

Lain noudattamisen valvonta

Lain noudattamista valvovana erityisviranomaisena toimisi Tietosuojavirasto. Tietosuojaviraston organisaatiosta säädettäisiin yleistä tietosuoja-asetusta täydentävässä laissa, jonka noudattamista se myös valvoisi. On tarkoituksenmukaista, että sama viranomainen valvoisi sekä yleisen tietosuoja-asetuksen, sitä täydentävän lain että direktiiviä täytäntöönpanevan lain noudattamista, ottaen huomioon että mainittu lain-säädäntö muodostaa varsin yhtenäisen kokonaisuuden. Henkilötietojen käsittelystä rikosasioissa annettuun lakiin otettaisiin säännökset Tietosuojaviraston tehtävistä ja toimivaltuuksista sen valvoessa kyseistä lakia.

Tietosuojavirasto valvoisi ehdotetun lain noudattamista sekä omatoimisesti että sille tehtyjen kanteluiden perusteella. Se voisi tehdä selvityksiä lain noudattamisesta ja käsittelee sille tehtyjä kanteluita. Virasto voisi lainvastaisen menettelyn tapauksessa esimerkiksi antaa rekisterinpitäjälle huomautuksen tai asettaa väliaikaisen tai pysyvän kiellon tai muun rajoituksen henkilötietojen käsittelylle. Virasto voisi asettaa oikeudellisesti velvoittavan päätöksensä tehosteeksi uhkasakon.

Tietosuojavirastolla olisi valvonnallisten tehtävien lisäksi ohjaavia ja henkilötietojen suojaa edistäviä tehtäviä. Sen tehtävänä olisi edistää yleistä tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, lainsäädännöstä, suojatoimista ja oikeuksista. Virasto myös antaisi pyynnöstä rekisteröidyille tietoja heidän oikeuksiensa käyttämisestä. Virasto edistäisi myös rekisterinpitäjien ja henkilötietojen käsittelijöiden tietoisuutta velvollisuuksistaan sekä antaisi näille neuvoja ennakkokuulemismenettelyssä.

Myös valtioneuvoston oikeuskansleri ja eduskunnan oikeusasiamies valvoisivat ehdotetun lainsäädännön noudattamista osana yleistä viranomaisten ja virkamiesten toiminnan laillisuusvalvontaa. Ne valvoisivat myös tuomioistuinten niiden lainkäyttötehtävien yhteydessä suorittamaa henkilötietojen käsittelyä, vaikka tuomioistuinten toiminnan valvomisen ei niiden lainkäyttötoiminnan osalta ehdoteta kuuluvan Tietosuojaviraston toimivaltaan.

Oikeusturva ja seuraamukset

Yleislakiin ehdotetaan otettavaksi säännökset toimivaltaisen viranomaisen velvollisuudesta ottaa käyttöön sellaiset menettelytavat, joita noudattamalla sille voidaan luottamuksellisesti ilmoittaa henkilötietojen suojan kannalta lainvastaisesta menettelystä. Tällaisilla matalan kynnyksen yhteydenottotavoilla (ns. whistleblowing-ilmiantojärjestelmä) rohkaistaisiin epäkohtia havaitsevia henkilöitä ilmoittamaan asiaa suoraan asianomaiselle viranomaiselle, jotta tämä voi oma-aloitteisesti ryhtyä asianmukaisiin korjaaviin tai muihin toimenpiteisiin.

Rekisteröidyn oikeusturvan kannalta käytännössä varsin keskeiseksi menettelyksi muodostuisi mahdollisuus kannella lainvastaiseksi epäilyistä menettelystä Tietosuojavirastolle. Kantelun voisi rekisteröidyn suostumuksella saattaa Tietosuojaviraston käsiteltäväksi myös yleishyödyllinen henkilötietojen suojaa edistävä yhteisö. Tietosuojaviraston tulisi tutkia kantelu tarpeellisin osin ja ilmoittaa kantelijalle kohtuullisen ajan kuluessa asian käsittelyn etenemisestä ja sen tuloksista. Virasto voisi edellä mainituin tavoin esimerkiksi kieltää henkilötietojen käsittelemisen. Viraston päätöksistä haettaisiin muutosta valittamalla hallinto-oikeuteen.

Direktiivin 56 artiklassa säädetyn mukaisesti jäsenvaltioiden on säädettävä rekisteröidyn oikeudesta saada korvausta siitä aineettomasta tai aineellisesta vahingosta, joka hänelle koituu lainvastaisesta menettelystä. Esityksessä ehdotetaan säädettäväksi, että rekisterinpitäjä on velvollinen korvaamaan sen taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle ehdotetun yleislain vastaisesta henkilötietojen käsittelystä. Rekisteröidylle voi myös syntyä mahdollisuus vaatia vahingonkorvauslaissa (412/1974) tarkoitettua niin sanottua kärsimyskorvausta. Vahingonkorvauslain 5 luvun 6 §:ssä säädetyn mukaan sillä, jonka yksityiselämää

on rangaistavaksi säädetyllä teolla loukattu, on oikeus korvaukseen loukkauksen aiheuttamasta kärsimyksestä.

Direktiivin 57 artiklassa säädetyn mukaisesti jäsenvaltioiden on vahvistettava säännöt tietosuojasäännösten rikkomisen johdosta määrättävistä tehokkaista, oikeasuhteisista ja varoittavista seuraamuksista. Yleinen tietosuoja-asetus puolestaan säättää siinä tarkoitettujen tietosuojasäännösten rikkomisista seuraamukseksi hallinnollisen seuraamusmaksun ("hallinnollisen sakon"), jonka käyttöalasta viranomaiset voidaan kuitenkin sulkea pois kokonaan tai osittain. Ehdotettuun yleislakiin otettaisiin viittaus-säännökset niihin rikoslain säännöksiin, jotka koskevat viestintäsalaisuuden loukkausta, tietomurtoa, vaitiolovelvollisuuden rikkomista ja virkarikoksia sekä näiden törkeitä tekemuotoja.

Esityksessä ei ehdoteta hallinnollisen seuraamusmaksun ottamista käyttöön ehdotetun yleislain soveltamisalalla. Tietosuojaviraston mahdollisuus antaa rekisterinpitäjää tai henkilötietojen käsittelijää koskevia oikeudellisesti sitovia määräyksiä sekä mahdollisuus tehostaa niitä uhkasakolla, rekisteröidyn oikeus saada korvaus kärsimästään vahingosta sekä rikoslain virkarikos- ja muu rangaistussäätely huomioon ottaen seuraamusmaksun käyttöönotto ei ehdotetun lain soveltamisalalla ole tarpeen. Esityksessä ehdotetaan direktiivin minimivaatimusta laajempia toimivaltuuksia Tietosuojavirastolle, mikä osaltaan mahdollistaisi laajemman keinovalikoiman puuttua lainvastaiseen henkilötietojen käsittelyyn. Rangaistusluonteisesta hallinnollisesta seuraamusmaksusta säätämistä viranomaistoiminnassa tapahtuvan lainvastaisen menettelyn seuraamukseksi ei myöskään voida pitää Suomen oikeusjärjestelmässä tavanomaisena ratkaisuna.

Euroopan komissio voi direktiivin 35 ja 36 artiklan mukaisesti tehdä päätöksen siitä, että jossakin kolmannessa maassa on henkilötietojen siirtämisen kannalta riittävä tietosuojan taso. Direktiivin 36 artiklassa säädetään muun muassa niistä seikoista, jotka komission tulee päätöstä tehdessään ottaa huomioon. Kansallinen valvontaviranomainen ei voi tutkia komission päätöksen lainmukaisuutta, sillä asia kuuluu EU-tuomioistuimen yksinomaiseen toimivaltaan.

Unionin tuomioistuin katsoi *Schrems*-tapauksessa (C-362/14) antamassaan ennakkoratkaisussa, että kansallisen lainsäätäjän asiana on säätää oikeussuojakeinoista, joiden avulla asianomainen kansallinen valvontaviranomainen voi esittää perusteltui-na pitämänsä perusteet kansallisissa tuomioistuimissa, jotta nämä voivat tarvittaessa pyytää ennakkoratkaisua Euroopan unionin tuomioistuimelta komission päätöksen pätevyyden tutkimiseksi. Näin ollen kansalliseen lainsäädäntöön on tarpeen sisällyttää säännökset tässä tarkoitettujen komission päätösten arvioimiseksi kansallisessa valvontaviranomaisessa ja tuomioistuimessa. Tämän vuoksi ehdotettuun yleislakiin otettaisiin säännökset siitä, että Tietosuojavirasto voi hakemuksella saattaa valvontaa

koskevan asian Helsingin hallinto-oikeuden ratkaistavaksi. Hallinto-oikeus puolestaan voisi tarvittaessa pyytää EU-tuomioistuimen ennakkoratkaisua komission päätöksen lainmukaisuudesta. Tällaisten asioiden käsitteleminen on tapausten oletettavan harvalukuisuuden vuoksi syytä keskittää Helsingin hallinto-oikeuteen.

Voimaantulo- ja siirtymäsäännökset

Ehdotettu yleislaki tulisi voimaan 6 päivänä toukokuuta 2018. Yleistä tietosuoja-asetusta ja sitä täydentävää kansallista lakia sovelletaan 25 toukokuuta 2018 alkaen. Tietosuojavirastoa koskevat organisaatiosäännökset on tarkoitus ottaa yleistä tietosuoja-asetusta täydentävään lakiin. Tästä johtuen esityksessä ehdotetaan, että tietosuojavaltuutettu valvoisi ehdotetun yleislain noudattamista siihen saakka, kunnes yleistä tietosuoja-asetusta täydentävä laki tulee voimaan.

Rikosasioiden tietosuojadirektiivin 63 artiklassa säädetään siitä, että jäsenvaltio voi lykätä edellä mainitun lokitusvelvollisuuden voimaantuloa enintään 6 päivään toukokuuta 2023 saakka, jos velvollisuudesta muutoin aiheutuisi suhteetonta vaivaa. Poikkeuksellisissa olosuhteissa ja jos velvollisuuden täyttämisestä aiheutuisi vakavia vaikeuksia kyseisen automaattisen käsittelyjärjestelmän toiminnalle, voidaan velvollisuuden voimaantuloa lykätä enimmillään 6 päivä toukokuuta 2026 asti. Mahdollisuus koskisi molemmissa tapauksissa ainoastaan sellaisia automatisoituja käsittelyjärjestelmiä, jotka on luotu ennen 6 päivää toukokuuta 2016. Ottaen huomioon, että Suomessa vain harva ennen 6 päivänä toukokuuta 2016 luotu tietojärjestelmä toteuttaa rikosasioiden tietosuojadirektiivin lokitusta koskevat vaatimukset, ja ottaen huomioon lokitusjärjestelmän luomisen edellyttämät ajalliset ja taloudelliset resurssit, esityksessä ehdotetaan säädettävän, että ennen 6 päivänä toukokuuta 2016 luodut järjestelmät on saatettava lokitetietoja koskevan sääntelyn mukaisiksi viimeistään 6 päivänä toukokuuta 2023.

Liitelait

Esitykseen sisältyy ehdotukset direktiivin kansallisen täytäntöönpanon edellyttämien muutosten tekemisestä eräisiin oikeusministeriön toimialan lakeihin. Kyseisistä laeista poistettaisiin viittaukset kumottavaan henkilötietolakiin, ja ne korvattaisiin tarpeen mukaan viittauksella ehdotettuun yleislakiin, yleiseen tietosuoja-asetukseen sekä tietosuojalakiin. Laeista poistettaisiin ehdotetun yleislain kanssa päällekkäistä sääntelyä esimerkiksi rekisteröidyn tarkastusoikeudesta. Eräiden lakien osalta selkeytettäisiin sitä, mitä viranomaista on pidettävä tietyn rekisterin osalta rekisterinpitäjänä.

6 Esityksen vaikutukset

6.1 Taloudelliset vaikutukset

Lakiehdotuksen taloudelliset vaikutukset kohdistuvat pääosin rekisterinpitäjinä toimiin toimivaltaisiin viranomaisiin. Ehdotetulla lailla ei ole juurikaan vaikutuksia yritysten toimintaan. Taloudelliset vaikutukset johtuvat pääsääntöisesti suoraan rikosasioiden tietosuojadirektiivistä.

Tietosuojavastaava. Rikosasioiden tietosuojadirektiivi edellyttää, että rekisterinpitäjä nimittää tietosuojavastaavan. Tästä aiheutuu välittömiä kustannuksia rekisterinpitäjille. Tietosuojavastaavien nimeämistä koskevan veloitteen suoria taloudellisia vaikutuksia alentaa se, että kaksi tai useampi rekisterinpitäjä voi nimetä yhteisen tietosuojavastaavan ja että tietosuojavastaava voi hoitaa sekä ehdotetusta laista että yleisestä tietosuoja-asetuksesta johtuvat tehtävät. Joillakin viranomaisilla, kuten poliisilla, on jo entuudestaan tietosuojavastaava, jolloin merkittäviä lisäkustannuksia ei pitäisi niille tältä osin syntyä.

Vaikutukset tietojärjestelmiin. Tietosuojadirektiivillä olisi suoria ja välillisiä vaikutuksia kansallisiin tietojärjestelmiin ja vaikutukset käytännössä konkretisoituvat yksittäisiä viranomaisia koskevan täydentävän sääntelyn kautta. Direktiivin vaatimusten kustannusvaikutukset voivat olla kokonaisuutena huomattavia siltä osin, kun kyse on pakollisista velvoitteista, joita ei ole aiemmin pantu täytäntöön tietojärjestelmissä. Kustannukset myös vaihtelevat rekisterinpitäjittäin.

Välittömiä ja välillisiä kustannusvaikutuksia voi olla erityisesti vaatimuksilla, jotka koskevat henkilöryhmien erottamista toisistaan järjestelmässä, aiempaa tiukemmat säännökset arkaluonteisten henkilötietojen käsittelystä, henkilökohtaiseen arvioon perustuvien henkilötietojen pitämistä mahdollisuuksien mukaan erillään varmoista henkilötiedoista, henkilötietojen käyttörajoitusmerkintöjä (rekisteröidyn taikka muun viranomaisen tai toisen jäsenvaltion viranomaisen pyynnöstä), lokitietoja ja erityisesti toimien perusteiden toteamista myös tietojen luovuttamisen perusteella, tietoturvallisuutta koskevia tarkennettuja vaatimuksia, pseudonymisoinnin laajempaa käyttöä ja tietojen poistamisvelvollisuuden ulottumista mahdollisesti varmuuskopioihin saakka.

Kustannusvaikutuksiltaan merkittävin tietojärjestelmiin kohdistuva vaatimus koskee lokijärjestelmiä. Esityksessä ehdotetaan, että lokijärjestelmien osalta otettaisiin käyttöön direktiivin sallima siirtymäaika, jonka mukaisesti tietojärjestelmien on oltava tältä osin vaatimustenmukaisia viimeistään 6 päivänä toukokuuta 2023. Muutoinkin

tietojärjestelmien uudistamisen täsmälliset kustannusvaikutukset riippuvat siitä, miten järjestelmiin kohdistuvat verraten väljät oikeudelliset vaatimukset päätetään toteuttaa käytännössä.

Poliisin tietojärjestelmät. Poliisilla on käytössä useita tietojärjestelmiä, jotka kuuluvat rikosasioden tietosuojadirektiivin soveltamisalaan. Rikosasioihin liittyvien henkilöryhmien tietojen erillään pitämistä koskeva velvollisuus perustuu osittain jo aiempaan Euroopan neuvoston suositukseen, samoin kuin velvollisuus erotella henkilökohtaiseen arvioon perustuvat tiedot varmennetuista tiedoista. Nämä velvollisuudet sisältävät myös jossain määrin joustoa. Poliisin tietojärjestelmissä vaatimukset toteutuvat pääosin, mutta joidenkin järjestelmien osalta kehittämistoimia voitaisiin toteuttaa. Poliisin uusissa tietojärjestelmissä vaatimus toteutettaisiin tarvittaessa uudistushankkeiden yhteydessä niiden toteutusaikataulun puitteissa.

Henkilötietojen käsittelyyn liittyvillä erityisillä edellytyksillä (informointivelvollisuudet, tietojen luovuttamiseen liittyvät rajoitukset) olisi välittömiä taloudellisia vaikutuksia. Myös siltä osin kuin on kyse henkilötietojen oikaisemisesta, poistamisesta ja käsittelyn rajoittamisesta, direktiivin vaatimusten toteuttaminen aiheuttaisi poliisin tietojärjestelmiin suoria kustannusvaikutuksia. Kaikkia tarvittavia toiminnallisuuksia ei ole toteutettu poliisin tietojärjestelmissä. Vaatimukset sisältyvät jo voimassa olevaan tietosuojapuitepäätökseen, joten lainsäädännön sisällöllinen muutos ei ole tältä osin kovin merkittävä. Osa vaatimuksista voisi kuitenkin olla teknisesti vaikeasti toteutettavissa tai jopa mahdotonta toteuttaa täysimääräisesti, ja kustannusvaikutukset voivat vaihdella kohtuullisista merkittäviin, riippuen direktiivin tulkinnasta ja valittavasta teknisestä toteutustavasta. Poliisin tietojärjestelmien osalta kustannusvaikutukset riippuvat siitä, miten tiukasti tulkitaan järjestelmäkyselyjen lokitietoja koskevaa vaatimusta. Kustannusvaikutukset voivat kuitenkin olla yksittäisen tietojärjestelmän osalta merkittäviä. Uusien järjestelmähankkeiden osalta lokitietoja koskevat velvoitteet olisi pantava huomioon niiden yhteydessä, huomioiden myös käytettävissä oleva siirtymäaika.

Oletetun ja sisäänrakennetun tietoturvallisuuden osalta kaikki poliisin olemassa olevat tietojärjestelmät on jo pyritty toteuttamaan siten, että niiden arvioidaan täyttävän direktiivin vaatimukset. Eräiden voimassa olevasta laista poikkeavien vaatimusten, jotka merkitsevät tiukempaa sääntelyä, arvioidaan kuitenkin aiheuttavan tarpeita muuttaa käytäntöjä siten, että niillä voi olla kustannusvaikutuksia. Nämä liittyvät erityisesti tietoturvaan ja niihin varautumiseen sekä henkilötietojen käsittelyyn liittyvään riskien arvioimiseen. Käsittelyn turvallisuuteen liittyvät vaatimukset on myös pääosin huomioitu poliisin tietojärjestelmissä. On kuitenkin mahdollista, että uhkakuviiin ja käsittelyn riskien arviointiin liittyvät vaatimukset aiheuttavat tietojärjestelmiin kohtuullisia muutostarpeita. Poliisin tietojärjestelmien osalta on arvioitu, että velvollisuudesta ilmoittaa tietoturvaloukkauksista toiselle viranomaiselle tai toiselle EU:n jäsenvaltion viranomaiselle mahdollisesti aiheutuu tarpeita toteuttaa muutostöitä.

Tulli. Tullin tietojärjestelmissä on sekä direktiivin että asetuksen soveltamisalaan liittyvää henkilötietojen käsittelyä. Tullissa rikosasioiden direktiivin soveltamisalaan kuuluvaa henkilötietojen käsittelyä suoritetaan suurelta osin poliisin ylläpitämissä teknisissä sovelluksissa (poliisiasiaain tietojärjestelmä ja epäiltyjen tietojärjestelmä). Tältä osin tietojärjestelmien direktiivinmukaisuudesta vastaa poliisi. Ehdotetun lain vaatimusten toteuttaminen ei alustavan arvion mukaan edellyttäisi järjestelmämuutoksia Tullin rekistereihin, eikä täten aiheuttaisi merkittäviä kustannuksia.

Rajavartiolaitos. Rajavartiolaitoksessa rikosasioiden direktiivin soveltamisalaan kuuluvaa henkilötietojen käsittelyä suoritetaan pääsääntöisesti poliisin ylläpitämissä teknisissä sovelluksissa (poliisiasiaain tietojärjestelmä ja epäiltyjen tietojärjestelmä). Tältä osin tietojärjestelmien direktiivinmukaisuudesta vastaa poliisi. Rikostorjunnan yksikkökohtaisten henkilörekisterien osalta on tarpeen arvioida, miltä osin nämä talletusalustat täyttävät ehdotetun täytäntöönpanolain vaatimukset, ja tehtävä tarvittavat muutokset joko talletusalustoihin tai yleisemmin henkilötietojen käsittelytapaan. Merkittävimmät selvitettävät asiat, joilla voi myös olla kustannusvaikutuksia, liittyvät henkilötietojen oikaisemista, poistamista ja käsittelyn rajoittamista sekä lokitietoja koskeviin vaatimuksiin. Ehdotetun lain muiden vaatimusten toteuttaminen ei alustavan arvion mukaan aiheuttaisi Rajavartiolaitoksessa merkittäviä kustannuksia, koska pääsääntöisesti vaatimukset toteutuvat jo nyt.

Puolustusvoimat. Puolustusvoimat uudistaa parhaillaan kaikkia isoja tietojärjestelmiään. Uudistustyö on aloitettu jo ennen EU:n tietosuojauudistusta, ja ehdotetusta laista arvioidaan aiheutuvat ainoastaan vähäisiä vaikutuksia Puolustusvoimien kehitysvaiheessa oleviin tietojärjestelmiin. Siirtymäajat huomioon ottaen, ehdotetusta laista seuraavat muutostarpeet eivät kuitenkaan vaadi lisärahoitusta. Tietosuojavastaavan kustannusvaikutus olisi Puolustusvoimille 1 henkilötyövuosi. Tämä vaikutus seuraisi osin ehdotetusta täytäntöönpanolaista ja osittain yleisestä tietosuojasetuksesta.

Oikeusministeriön hallinnonala. Oikeusrekisterikeskuksen tietojärjestelmiin (rikosrekisteri, sakon täytäntöönpanoa koskeva järjestelmä Rajsa ja rikosrekisteritietojen EU-tiedonvaihtoon käytettävästä CRIS-järjestelmästä) olisi tehtävä ehdotetun lain johdosta muutoksia. Kuluja syntyisi esimerkiksi lakiehdotuksen mukaisesta lokitusvelvollisuudesta ja korkeammista tietoturva vaatimuksista. Arvio edellä mainittuihin järjestelmiin vaadituista muutoksista aiheutuvista kertaluonteisista kuluista on 500 000–600 000 euroa ja jatkuvien palveluiden lisäkustannukset 20 000–40 000 euroa vuodessa. Merkittävimmät kustannusvaikutukset syntyisivät tietojen lokitusvelvollisuuden toteuttamisesta sakon täytäntöönpanojärjestelmään.

Ehdotetusta laista seuraisi myös muita vaikutuksia oikeusministeriön hallinnonalan tietojärjestelmiin kuten esimerkiksi Rikosseuraamuslaitoksen tietojärjestelmiin. Syyttäjien ja tuomioistuinten käyttämään Sakari-järjestelmään olisi niin ikään tehtävä muu-

toksia ehdotetun lain johdosta. Erityisesti lokitusvelvollisuuden toteuttamisesta aiheutuu mainitun järjestelmän osalta merkittäviä kustannusvaikutuksia.

6.2 Vaikutukset viranomaisten toimintaan

EU:n tietosuojalainsäädännön uudistaminen merkitsee hallinnollisen taakan kasvua rekisterinpitäjille. Hallinnollista taakkaa aiheutuisi potentiaalisesti siitä, että tietosuoja sääntelyä koskevan tietoisuuden lisääntymisen ja aiempaa vahvempien valvontaviranomaisten toimivaltuuksien myötä rekisteröidyt henkilöt käyttäisivät aiempaa aktiivisemmin oikeuksiaan. Sitä, missä määrin rekisteröidyt käyttäisivät oikeuksiaan, on kuitenkin vaikea arvioida. Kustannusvaikutukset liittyisivät pääosin tietosuojavaikuttavien tehtävien hoitoon, mutta mahdollisesti myös rekisterinpitäjän edustamiseen hallinto-oikeudellisissa ja rikosoikeudellisissa menettelyissä. Ottaen huomioon, että rekisteröidyn oikeuksia on tehostettu myös EU:n laajuisesti huomioimalla sääntelyssä nimenomaisesti oikeussuojakeinojen käyttö myös rajat ylittävissä tilanteissa ja laajentamalla tietosuojavaikuttavien toimivaltuuksia EU:n laajuisesti, rekisterinpitäjät joutuvat mahdollisesti varautumaan näiden oikeuksien käyttöön myös resursoinnilla.

Toisaalta osa velvollisuuksista sisältyy jo voimassa olevaan sääntelyyn, joten kokonaisvaikutusta voidaan tältä osin pitää kohtuullisena. Rekisterinpitäjän olisi kuitenkin esimerkiksi laadittava tietosuojavaikutusten arviointi uusista henkilötietojen käsittelytoimenpiteistä, mikä ei nimenomaisena velvollisuutena sisälly voimassa olevaan sääntelyyn. Rekisterinpitäjälle aiheutuisi hallinnollista taakkaa lisäksi henkilötietojen käsittelijöiden sitouttamisesta uusiin vaatimuksiin sopimuksia uusimalla. EU:n tietosuojalainsäädännössä huomioidaan aiempaa yksityiskohtaisemmin rekisterinpitäjän ja henkilötietojen käsittelijöiden suhde ja keskinäiset velvollisuudet.

Ehdotetusta laista aiheutuisi vaikutuksia kansalliselle valvontaviranomaiselle eli Tietosuojavirastolle. Vaikutukset olisivat kuitenkin jokseenkin maltillisia verrattuna yleisestä tietosuoja-asetuksesta seuraavista vaikutuksista. Taloudellisia vaikutuksia synnyisi etenkin ehdotetun lain mukaisista uusista tehtävistä. Näitä olisivat 21 §:n mukainen ennakkokuulemismenettely, tiedottaminen ja neuvontatyö etenkin lain tullessa voimaan, 29 §:n mukaisen välillisen tarkastusoikeuden käyttö Tietosuojaviraston välityksellä, 34 §:n mukaisten tietoturvaloukkausten käsittely sekä osallistuminen tietosuojavaikuttavien keskinäiseen avunantoon ja kansainväliseen yhteistyöhön. Tällä hetkellä rikosasioiden tietosuojadirektiivin toimialaan kuuluviin tehtäviin käytetään tietosuojavaikuttavien toimistossa noin 1,5 henkilötyövuotta. Lisäresurssien tarpeen arvioidaan olevan 2 henkilötyövuotta, minkä lisäksi viraston yleiskustannuksiin (esimerkiksi julkaisutoiminta) on tarpeen osoittaa lisämäärärahoja viraston toiminnan

vaikuttavuuden vahvistamiseksi. Lisäresurssien tarpeen arvioidaan siten olevan vuositasolla yhteensä 200 000 € (2 x 80 000 € + 40 000 €).

6.3 Yhteiskunnalliset vaikutukset

Rikosasioiden tietosuojadirektiivin tavoitteena on helpottaa henkilötietojen vapaata kulkua toimivaltaisten viranomaisten kesken EU:ssa rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten ja tällaisten tietojen siirtämistä kolmansiin maihin ja kansainvälisille järjestöille. Toisaalta samalla on pyritty varmistamaan henkilötietojen entistä vahvempi ja johdonmukaisempi suoja, jota tuetaan tehokkaalla täytäntöönpanolla.

Euroopan komissio on omassa EU-tason vaikutustenarvioinnissaan kiinnittänyt huomiota siihen, että aiempaa yhtenäisempi ja yksityiskohtaisempi rikosasioihin liittyvää henkilötietojen käsittelyä koskeva sääntely EU:n laajuisesti selkiyttää oikeustilaa ja parantaa yritysten luottamusta poliisin henkilötietojen käsittelyyn. Tällä komissio on arvioinut olevan merkitystä erityisesti niissä tilanteissa, joissa lainvalvontaviranomainen on suoraan yhteydessä EU:n alueella toimiviin yrityksiin saadakseen tai luovuttaakseen henkilötietoja rajat ylittävien palvelujen tarjonnan tilanteisiin liittyen. Toisaalta pitkällä aikavälillä uusi tietosuojasääntely kuitenkin kannustaa kehittämään tietojärjestelmiä varmemmiksi ja tietoturvalisemmiksi. Lisäksi rekisterinpitoa ja rekisterien valvontaa koskevalla aiempaa yksityiskohtaisemmalla sääntelyllä ja uusilla hallinnollisilla seuraamuksilla voidaan arvioida olevan tietosuojarikkomusten ja tietoturvallisuusloukkausten riskejä vähentävää vaikutusta.

Tietosuojapuitepäätöksen osalta pääasialliset komission esiin nostamat ongelmat liittyvät säädöksen rajalliseen soveltamisalaan ja muihin aukkoihin sääntelyssä. Nämä konkretisoituvat komission arvion mukaan, kun EU:n sisäinen ja EU:n rajat ylittävä kansainvälinen yhteistyö lisääntyy. Sääntelyä on myös pidetty hajanaisena, ottaen huomioon erot tietosuojapuitepäätöksen täytäntöönpanossa. Puitepäätöksen korvaavassa tietosuojadirektiivissä on pyritty poistamaan sääntelyn hajanaisuutta siten, että soveltamisala laajenee koskemaan kaikkea rikosasioihin liittyvää henkilötietojen käsittelyä riippumatta siitä, onko kyse rajat ylittävästä henkilötietojen siirrosta vai kansallisesta käsittelystä. Komission tavoitteena on ollut varmistaa, että yksilön oikeudet taa-taan täysimääräisesti, sekä samalla parantaa luottamusta poliisiyhteistyöhön ja helpottaa sitä. Uudella direktiivillä on myös pyritty varmistamaan yhtenäisten ja johdonmukaisten periaatteiden soveltaminen kaikkeen henkilötietojen käsittelyyn. Samat vaatimukset on huomioitava myös kansainvälisissä henkilötietojen siirroissa.

7 Asian valmistelu

Sisäministeriö, puolustusministeriö ja valtiovarainministeriö asettivat vuonna 2016 hankkeet rikosasioiden tietosuojadirektiivin täytäntöönpanemiseksi kunkin hallinnonalalla. Ministeriöiden välisissä keskusteluissa kuitenkin havaittiin, että rikosasioiden tietosuojadirektiivi sisältää pääosin sellaista yleistä sääntelyä, joka on direktiivin kansallisessa täytäntöönpanossa perusteltua koota yhteen yleislakiin. Yleislakia sovellettaisiin kaikilla direktiivin soveltamisalaan kuuluvilla hallinnonaloilla, jolloin vältetään päällekkäiseltä hallinnonalakohtaiselta sääntelyltä ja mahdollisilta perusteettomilta lainsäädännön eroavuuksilta. Henkilötietojen käsittelyä koskevien erillislakien tarpeelliset viranomaisten rekisterijärjestelmiä sekä muuta tietojenkäsittelyä koskevat muutokset on valmisteltu erikseen kullakin hallinnonalalla siten, että hallituksen esitykset voidaan antaa mahdollisimman yhtäaikaaisesti eduskunnan käsiteltäväksi.

Oikeusministeriö asetti 12.1.2017 työryhmän, jonka tehtävänä oli valmistella ehdotus tarpeelliseksi yleiseksi lainsäädännöksi rikosasioiden tietosuojadirektiivin täytäntöönpanemiseksi samoin kuin ehdotukset direktiivin edellyttämistä muutoksista oikeusministeriön hallinnonalan lainsäädäntöön. Työryhmän tuli myös selvittää, voidaanko puheena olevaa yleistä lainsäädäntöä soveltaa sellaiseen toimintaan, joka jää tietosuojadirektiivin ja tietosuoja-asetuksen soveltamisalan ulkopuolelle, mutta jonka sääntely on perusteltua sovittaa yhteen turvallisuusviranomaisia koskevan muun sääntelyn kanssa. Työryhmässä olivat edustettuina oikeusministeriö, sisäministeriö, puolustusministeriö, valtiovarainministeriö, tietosuojavaltuutettu, Oikeusrekisterikeskus ja Valtakunnansyyttäjänvirasto.

Työryhmän toimikausi oli 16.1.–29.9.2017.

8 Riippuvuus muista esityksistä

Esityksellä on yhteys valmisteilla olevaan esitykseen yleistä tietosuoja-asetusta täydentäväksi kansalliseksi lainsäädännöksi. Oikeusministeriö asetti helmikuussa 2016 TATTI-työryhmän (OM006:00/2016), jonka tehtävänä oli valmistella yleisen tietosuoja-asetuksen edellyttämiä muutoksia henkilötietojen käsittelystä annettuun yleiseen kansalliseen lainsäädäntöön. Työryhmän tehtävänä oli erityisesti valmistella ehdotus kansallista tietosuojaviranomaista koskevaksi sääntelyksi. Työryhmä luovutti mietintönsä 21.6.2017, jonka jälkeen mainitun lainsäädännön valmistelu on jatkunut virkatyönä oikeusministeriössä. Esityksellä on lisäksi yhteys Ahvenmaan maakuntahallituksen selvitystyöhön yleisestä tietosuoja-asetuksesta ja rikosasioiden tietosuojadirektiivistä seuraavista muutostarpeista.

Esitys liittyy sisäministeriön asettaman työryhmän (SM064:00/2015) työhön, jossa on tarkoitus laatia ehdotus hallituksen esitykseksi laiksi henkilötietojen käsittelystä poliisi-toiminnassa. Hankkeen keskeisin tavoite on valmistella uusi poliisin henkilötietolaki, joka täydentäisi rikosasioiden tietosuojadirektiivin yleistä täytäntöönpanolainsäädäntöä ja yleistä tietosuoja-asetusta siltä osin kuin tarvittavat täytäntöönpanosäännökset eivät sisälly mainittuihin säädöksiin. Tarkoituksena on, että uusi poliisin henkilötietolaki täyttäisi uudistuneen EU:n tietosuojalainsäädännön vaatimukset, ottaen huomioon rikostorjunnan tarpeet ja perus- ja ihmisoikeuksien asettamat vaatimukset. Mainittua lainsäädäntöä koskeva hallituksen esitys on tarkoitus antaa eduskunnalle samanaikaisesti tämän esityksen kanssa.

Esityksellä on yhteys sisäministeriön asettaman työryhmän (SM057:00/2016) työhön, jossa tehtävänä on laatia hallituksen esitys henkilötietojen käsittelyä Rajavartiolaitoksessa koskevan lainsäädännön tarkistamiseksi. Hankkeessa valmistellaan muutokset henkilötietojen käsittelystä rajavartiolaitoksessa annettuun lakiin siltä osin, kun tarvittavat säännökset eivät sisälly rikosasioiden tietosuojadirektiivin kansalliseen täytäntöönpanolakiin. Lisäksi työryhmä arvioi muut EU:n uudistuneesta tietosuojalainsäädännöstä seuraavat lain muutostarpeet sekä tarkistaa meripelastuslain henkilötietojen käsittelyä koskevat säännökset. Mainittua lainsäädäntöä koskeva hallituksen esitys on tarkoitus antaa eduskunnalle samanaikaisesti tämän esityksen kanssa.

Esitys liittyy valtiovarainministeriön asettaman työryhmän (VM059:00/2016) työhön, jossa on tarkoitus muuttaa henkilötietojen käsittelystä Tullissa annettua lakia vastaamaan yleistä tietosuoja-asetusta ja rikosasioiden tietosuojadirektiiviä siltä osin kuin jälkimmäisestä seuraavat muutostarpeet eivät tule katetuksi rikosasioiden tietosuojadirektiivin yleisellä täytäntöönpanolainsäädännöllä. Mainittua lainsäädäntöä koskeva hallituksen esitys on tarkoitus antaa eduskunnalle samanaikaisesti tämän esityksen kanssa.

Esitys liittyy niin ikään puolustusministeriön asettaman työryhmän (PLM006:00/2016) työhön, jossa valmistellaan henkilötietojen käsittelyä puolustushallinnossa koskevan lainsäädännön kokonaisuudistusta. Työryhmän tehtävänä on selvittää henkilötietojen käsittelyä puolustushallinnossa koskevan lainsäädännön EU:n tietosuojauudistuksesta seuraavat muutostarpeet ja valmistella ehdotus tarvittaviksi säädösmuutoksiksi. Mainittua lainsäädäntöä koskeva hallituksen esitys on tarkoitus antaa eduskunnalle samanaikaisesti tämän esityksen kanssa.

YKSITYISKOHTAISET PERUSTELUT

9 Lakiehdotusten perustelut

9.1 Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä

1 luku Yleiset säännökset

1 §. *Soveltamisala.* Pykälässä säädettäisiin ehdotetun lain soveltamisalasta. Rikosasioiden tietosuojadirektiivin soveltamisalasta säädetään sen 1 ja 2 artiklassa, joihin myös ehdotettu soveltamisalasäännös pääosin perustuisi.

Pykälän 1 *momentin* mukaan ehdotettua lakia sovellettaisiin laissa määriteltyjen toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kyse on rikoksen ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta (1 kohta), syyteharkinnasta ja muusta rikokseen liittyvästä syyttäjän toiminnasta (2 kohta), rikosasian käsittelemisestä tuomioistuimessa (3 kohta), rikosoikeudellisen seuraamuksen täytäntöönpanemisesta (4 kohta) taikka yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä kohdassa 1–4 tarkoitettun toiminnan yhteydessä (5 kohta).

Rikosasioiden tietosuojadirektiivin johdanto-osan 12 kappaleen mukaan poliisiviranomaisten tai muiden lainvalvontaviranomaisten suorittamat toimet keskittyvät lähinnä rikosten ennalta estämiseen, tutkimiseen, paljastamiseen tai rikoksiin liittyviin syyte-toimiin, mukaan lukien poliisin toimet, jotka koskevat häiriöitä, joista ei ennakoon tiedetä, onko kyse rikoksesta. Tällaisiin toimiin voi kuulua vallan käyttö toteuttamalla pakkokeinoja, kuten mielenosoituksissa, suurissa urheilutapahtumissa ja mellakoissa

toteutetut poliisin toimet. Mainittuihin toimiin kuuluu myös lain ja järjestyksen ylläpitäminen, joka on annettu poliisiviranomaisten tai muiden lainvalvontaviranomaisten tehtäväksi silloin, kun se on tarpeen sellaisilta yleiseen turvallisuuteen ja yhteiskunnan perustavanlaatuisiin lailla suojattuihin etuihin kohdistuvilta uhkilta suojelua ja niiden ehkäisyä varten, jotka voivat johtaa rikokseen.

Ehdotetussa laissa tarkoitettuja toimivaltaisia viranomaisia ovat ainakin poliisi- ja tulliviranomaiset ja Rajavartiolaitos, tuomioistuimet, ulosottoviranomaiset, syyttäjälaitos, Oikeusrekisterikeskus sekä Rikosseuraamuslaitos. Lisäksi esimerkiksi eduskunnan oikeusasiamies ja oikeuskansleri voivat olla lain tarkoittamia toimivaltaisia viranomaisia, sillä niillä on perustuslain 110 §:ssä säädetyn mukaisesti syyteoikeus. Ehdotettua lakia sovellettaisiin toimivaltaisiin viranomaisiin kuitenkin ainoastaan siltä osin, kun ne suorittavat henkilötietojen käsittelyä lain 1 §:n 1 momentissa lueteltuja tehtäviä varten.

Toimivaltaisille viranomaisille voidaan kansallisessa lainsäädännössä antaa sellaisia-kin tehtäviä, joita ei suoriteta rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia varten eikä yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten. Tällöin siltä osin kuin näitä muita tarkoituksia varten suoritettava henkilötietojen käsittely kuuluu unionin oikeuden soveltamisalaan, kuuluu kyseinen toiminta asetuksen (EU) 2016/679 eli niin sanotun yleisen tietosuoja-asetuksen soveltamisalaan.

Esimerkiksi poliisilla on useita tietosuojadirektiivin ja ehdotetun lain soveltamisalaan kuuluvia tehtäviä, kuten rikosten esitutkinta. Se kuitenkin hoitaa muitakin kuin lainvalvontaan liittyviä tehtäviä esimerkiksi käsitellessään passihakemuksia. Tällaiseen käsittelyyn ei sovellettaisi ehdotettua lakia, vaan yleistä tietosuoja-asetusta ja sitä täydentävää kansallista lainsäädäntöä. Niin ikään lain soveltamisalaan ei kuuluisi henkilötietojen käsittely henkilöstöhallinnossa, turvapaikka-asiat, maahanmuutto, rajavaltiota, tai pankkien suorittama henkilötietojen käsittely. Näitä asioita ja tilanteita koskevat käsittelytoimet kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan.

Lisäksi esimerkiksi Tullille säädettyistä tehtävistä rikosasioiden tietosuojadirektiivin ja ehdotetun lain soveltamisalaan kuuluisivat tullirikosten estäminen ja paljastaminen sekä niiden esitutkinnan suorittaminen. Lain soveltamisalaan eivät kuuluisi Tullille säädettyistä tehtävistä esimerkiksi EU:n tullilainsäädännön toimeenpanoon liittyvät tehtävät, verotuksen toimittaminen, valvontatehtävät, ulkomaankaupan tilastointi ja laboratoriotutkimukset, vaan näiden osalta sovellettavaksi tulisi yleinen tietosuoja-asetus.

Pykälän 2 momentin 1 kohdan mukaan lakia sovellettaisiin lisäksi sellaiseen Puolustusvoimien suorittamaan ja Puolustusvoimien lukuun suoritettavaan henkilötietojen käsittelyyn, jota suoritetaan puolustusvoimista annetun lain 2 §:n 1 momentin maini-

tuissa kohdissa säädettyjen tehtävien suorittamiseksi. Kohdassa tarkoitettu henkilötietojen käsittely ei kuulu rikosasioiden tietosuojadirektiivin soveltamisalaan, eli kyseessä olisi kansallinen lain soveltamisalan laajennus.

Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdassa säädetään Puolustusvoimien päätehtävästä, joka on Suomen sotilaallinen puolustaminen. Kohta jakaantuu kolmeen alakohtaan, joissa säädetään tarkemmin tehtävän sisällöstä.

Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan a alakohdassa säädetään Puolustusvoimien tehtäväksi Suomen maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen. Valtakunnan alueellisen koskemattomuuden turvaamiseksi valtakunnan maa- ja merialuetta sekä ilmatilaa valvotaan yhteistoiminnassa muiden valvontaviranomaisten kanssa. Aluevalvonnalla ehkäistään tai paljastetaan ja selvitetään aluerikkomukset ja alueloukkaukset. Puolustusvoimien osallistumisesta maa- ja vesialueen sekä ilmatilan valvontaan säädetään tarkemmin aluevalvontalaissa.

Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan b alakohdan mukaan Suomen sotilaalliseen puolustamiseen kuuluu lisäksi kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen sekä laillisen yhteiskuntajärjestyksen puolustaminen. Sotilaallisen uhan ennalta ehkäisemiseksi on puolustusvoimien valmiutta pystyttävä kohottamaan, kutsumaan tarvittavat joukot palvelukseen, hajauttamaan sodan ajan joukkojen materiaali ja suojaamaan tärkeät kohteet. Puolustusvoimat siten ylläpitää ja kehittää puolustusvalmiutta. Sotilasstrategisen tilannekuvan muodostamiseksi ja ylläpitämiseksi tiedustelu- ja valvontajärjestelmä seuraa Suomen turvallisuussympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta. Järjestelmä antaa ennakkovaroituksen sotilaallisten uhkien kehittymisestä, jotta voidaan käynnistää tarvittavat vastatoimenpiteet. Puolustusvalmiuden ylläpitäminen ja kehittäminen sisältää myös muun muassa puolustusmateriaalin hankintaa, huoltoa, varastointia, logistiikkaa, operatiivista suunnittelua, johtamisjärjestelmien kehittämistä, henkilöstön kouluttamista, valmiuden säätelyä, valmiusyhtymien kehittämistä ja tietosodankäyntiin valmistautumista.

Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan c alakohdassa säädetään Puolustusvoimien tehtäväksi sotilaskoulutuksen antaminen, vapaaehtoisen maanpuolustuskoulutuksen ohjaaminen ja maanpuolustustahdon edistäminen. Puolustusvoimat tuottaa kansallisen puolustuksen joukot. Tämän vuoksi puolustusvoimat antaa sotilaskoulutusta varusmiehille, reserviläisille ja sotilasoppilaitoksissa opiskeleville. Puolustusvoimat myös tukee vapaaehtoista maanpuolustusta osana Suomen puolustusta siten kuin vapaaehtoisesta maanpuolustuksesta annetussa laissa (556/2007) säädetään. Puolustusvoimat edistää maanpuolustustahtoa esimerkiksi antamalla kansalaisille mahdollisuuksia osallistua maanpuolustustyöhön sekä sitouttamalla kansalaisia

niihin arvoihin ja toimintoihin, jotka edistävät maanpuolustusta. Myös yhteistyö veteraanijärjestöjen ja vastaavien kanssa liittyy maanpuolustustahdon edistämiseen.

Mainitun pykälän 1 momentin 2 kohdan mukaan puolustusvoimien tehtävänä on muiden viranomaisten tukeminen. Tehtävään kuuluvat a) virka-apu yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, terrorismirikosten estämiseksi ja keskeyttämiseksi sekä muuksi yhteiskunnan turvaamiseksi sekä b) pelastustoimintaan osallistuminen antamalla käytettäväksi pelastustoimintaan tarvittavaa kalustoa, henkilöstöä ja asiantuntijapalveluja. Ehdotettua lakia sovellettaisiin vain a alakohdan mukaisten tehtävien hoitamisen yhteydessä.

Puolustusvoimien tukea muille viranomaisille tarvitaan tilanteissa, joissa muilla viranomaisilla ei ole esimerkiksi puolustusvoimilta löytyvää osaamista tai kalustoa tehtävien suorittamiseen. Yhteistoiminnan taustalla ovat lakisääteiset velvoitteet sekä viranomaisten väliset yhteistoimintasopimukset. Perinteisten sotilaallisten uhkien lisäksi muun muassa joukkotuhoaseuhka, terrorismi, informaationsodankäynti sekä tietojärjestelmiin kohdistuvat uhkat ovat haasteita, joita puolustusvoimat seuraa huolellisesti. Normaaliajan yhteistoiminnalla luodaan perusteet niin häiriötilanteiden kuin myös poikkeusolojen kiinteää ja toimivaa yhteistoimintaa varten.

Puolustusvoimien kolmantena tehtävänä on osallistuminen Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklaan tai Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohtaan perustuvaan apuun, aluevalvontayhteistyöhön tai muuhun kansainvälisen avun antamiseen ja kansainväliseen toimintaan a) virka-apu yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, terrorismirikosten estämiseksi ja keskeyttämiseksi sekä muuksi yhteiskunnan turvaamiseksi. Kansainvälistä apua voidaan säännöksen nojalla antaa toiselle valtiolle, Euroopan unionille tai kansainväliselle järjestölle esimerkiksi EU:n yhteisvastuulausekkeen tai keskinäisen avunannon lausekkeen tilanteissa taikka aluevalvonnassa. Esimerkkeinä säännöksessä tarkoitettu muusta kansainvälisestä toiminnasta voidaan mainita Suomen omista tarpeista lähtevä yhteistoiminta esimerkiksi aluevalvonnassa alueella, joka ei kuulu minkään valtion suvereniteettiin kuten aavalla merellä tai kansainvälisessä ilmatilassa taikka suomalaisten evakuointi kriisialueelta Puolustusvoimien suorituskykyä käyttämällä.

Puolustusvoimien neljäntenä tehtävänä on osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan ja sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa. Sotilaalliseen kriisinhallintaan osallistumisesta säädetään tarkemmin sotilaallisesta kriisinhallinnasta annetussa laissa.

Ehdotetun pykälän 2 momentin 2 kohdan mukaan lakia sovelletaan poliisin suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään poliisilain 1 §:n 1 momentissa tarkoitettussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen. Poliisi-

lain 1 luvun 1 §:n 1 momentin mukaan poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä. Suojelupoliisin tehtävänä on poliisin hallinnosta annetun lain (110/1992) 10 §:n mukaan torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi.

Suojelupoliisin käsitellessä henkilötietoja tehtävänsä suorittamiseksi eli kansallisen turvallisuuden suojaamiseksi, sen henkilötietojen käsittely ei kuulu EU:n oikeuden alaan. Kansallinen turvallisuus on Euroopan unionista tehdyssä sopimuksessa suljettu EU:n toimivallan ulkopuolelle. Tästä syystä kansallisen turvallisuuden perusteella käsiteltävistä henkilötiedoista on säädettävä kansallisessa lainsäädännössä. Ehdotettua lakia sovellettaisiin myös muun poliisin yksikön suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään poliisilain 1 §:n 1 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen.

Pykälän 2 momentin 3 kohdan mukaan lakia sovellettaisiin Rajavartiolaitoksen henkilötietojen käsittelyyn, kun tietoja käsitellään kansallisen turvallisuuden suojaamisen yhteydessä. Rajavartiolain 3 §:ssä säädetään Rajavartiolaitoksen tehtävistä. Kansallisen turvallisuuden suojaamiseen niistä liittyvät erityisesti eräät valvontatehtävät sekä sotilaallisen maanpuolustuksen tehtävät. Rajavartiolain 3 §:n 2 momentin mukaan Rajavartiolaitos suorittaa sille erikseen säädettyjä valvontatehtäviä, joihin kuuluu muiden muassa Suomen alueellisen koskemattomuuden valvonta ja turvaaminen. Rajavartiolaitos huolehtii aluevalvonnasta yhteistyössä puolustusvoimien ja muiden aluevalvontaviranomaisten kanssa siten kuin aluevalvontalaissa säädetään. Rajavartiolain 3 §:n 3 momentin mukaan Rajavartiolaitos osallistuu sotilaalliseen maanpuolustukseen. Rajavartiolain 25 §:n 1 momentin mukaan Rajavartiolaitos antaa tässä tarkoituksessa henkilöstölleen ja Rajavartiolaitoksen palvelukseen määrätyille asevelvollisille samoin kuin vapaaehtoisesti asepalvelusta suorittamaan otetuille naisille sotilas-koulutusta sekä ylläpitää ja kehittää puolustusvalmiutta yhteistoiminnassa puolustusvoimien kanssa.

Pykälän 3 *momentin* mukaan 2 momentissa tarkoitettuun henkilötietojen käsittelyyn ei kuitenkaan sovellettaisi henkilötietojen luovuttamista kolmansiin maihin koskevaa 7 lukua. Henkilötietojen vapaa liikkuvuus unionin alueella ei koske ehdotetun 2 momentin soveltamisalalla tapahtuvaa henkilötietojen käsittelyä, eikä esimerkiksi erottelu unionin jäsenvaltioiden ja kolmansien maiden välillä ole siten tältä osin merkityksellinen.

Pykälän *4 momentin* mukaisesti ehdotettua lakia sovellettaisiin kuitenkin vain sellaiseen 1 ja 2 momentissa tarkoitettuun henkilötietojen käsittelyyn, joka on kokonaan tai osittain automaattista tai jossa käsiteltävät tiedot muodostavat tai niiden on tarkoitus muodostaa rekisteri tai sen osa. Lain soveltamisalaan kuuluisivat siten myös manuaaliset rekisterit, eikä ehdotuksessa ole tarkoitus tältä osin muuttaa nykyistä henkilötietolaissa säädettyä oikeustilaa.

Pykälän *5 momentti* sisältäisi informatiivisen säännöksen siitä, että ehdotetulla lailla pannaan täytäntöön rikosasioiden tietosuojadirektiivi.

2 §. Suhde muuhun lainsäädäntöön. Pykälän *1 momentissa* säädettäisiin selvyiden vuoksi, että jos muussa laissa on tässä ehdotetusta laista poikkeavia säännöksiä, niitä sovelletaan tämän lain asemesta. Käytännössä lähes jokaista toimivaltaista viranomaista ja sen suorittamaa henkilötietojen käsittelyä koskevaa erityislainsäädäntöä on olemassa, jolloin kyseisiä säännöksiä sovellettaisiin ensisijaisesti suhteessa tähän lakiin.

Pykälän *2 momentti* sisältäisi informatiivisen viittaussäännökseen viranomaisten toiminnan julkisuudesta annettuun lakiin. Nykytilaa vastaavasti oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista säädettäisiin ehdotetun lain sijaan julkisuuslaissa. Luovutettaessa henkilötietoja viranomaisten tulee ottaa huomioon julkisuusperiaate ja salassapitosäännökset siten kuin perustuslain 12 §:n 2 momentissa, julkisuuslaissa ja mahdollisesti soveltuvassa erityislainsäädännössä säädetään.

Rikosasioiden tietosuojadirektiivin johdanto-osan 16 kappaleen mukaan direktiivi ei rajoita virallisten asiakirjojen julkisuusperiaatetta. Lisäksi yleisen tietosuoja-asetuksen mukaan viranomaiset tai julkis- tai yksityisoikeudelliset yhteisöt voivat luovuttaa viranomaisten tai yhteisöjen hallussa yleisen edun vuoksi toteutetun tehtävän suorittamiseksi olevien virallisten asiakirjojen sisältämiä henkilötietoja sellaisen unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti, jota viranomaiseen tai yhteisöön sovelletaan, jotta voidaan sovittaa yhteen virallisten asiakirjojen julkisuus ja oikeus henkilötietojen suojaan.

3 §. Määritelmät. Pykälässä määriteltäisiin ehdotetun lain keskeiset käsitteet. Pykälä perustuu rikosasioiden tietosuojadirektiivin 3 artiklaan.

Pykälän *1 momentin 1 ja 2 kohdassa* määriteltäisiin henkilötieto, rekisteröity ja henkilötietojen käsittely. Määritelmien sisältö ei muuttuisi nykylainsäädännöstä, mutta mää-

ritelmien kirjoitusasua päivitettäisiin vastaamaan paremmin rikosasioiden tietosuojadirektiivissä ja yleisessä tietosuojasetuksessa käytettyjä määritelmiä. Henkilötiedoilla tarkoitettaisiin kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön välittömästi tai välillisesti liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai välillisesti tunnistaa erityisesti nimen, henkilötunnuksen tai yhden tai useamman hänelle tunnusomaisen fyysisen, geneettisen tai esimerkiksi sosiaalisen tekijän perusteella.

Momentin 3 kohdan sisältämä käsite *käsittelyn rajoittaminen* olisi uusi. Sillä tarkoitettaisiin tallennettujen henkilötietojen merkitsemistä siten, että tarkoituksena on rajoittaa tietojen myöhempää käsittelyä.

Momentin 4 kohdan sisältämä käsite *rekisteri* vastaisi henkilötietolaissa käytettyä henkilörekisterin käsitettä. Määritelmä yhdenmukaistettaisiin rikosasioiden tietosuojadirektiivin määritelmäsäännöksen kanssa, ja rekisterillä tarkoitettaisiin mitä tahansa jäsenneiltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, riippumatta siitä, onko tietojoukko keskitetty, hajautettu taikka toiminnallisin tai maantieteellisin perustein jaettu.

Momentin 5 kohdassa määriteltäisiin *toimivaltainen viranomainen*. Sillä tarkoitettaisiin kaikkia sellaisia viranomaisia, joiden toimivalta kattaa rikosten ennalta estämisen, paljastamisen, selvittämisen tai syyteharkintaan saattamisen, rikosoikeudellisiin seuraamuksiin tuomitsemisen tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy. Kohdassa tarkoitettuja toimivaltaisia viranomaisia olisivat ainakin poliisi- ja tulliviranomaiset, Rajavartiolaitos, tuomioistuimet, ulosottoviranomaiset, syyttäjälaitos, Oikeusrekisterikeskus sekä Rikosseuraamuslaitos. Lisäksi esimerkiksi eduskunnan oikeusasiamies ja oikeuskansleri voivat olla lain tarkoittamia toimivaltaisia viranomaisia, sillä niillä on tietyissä tilanteissa syyteoikeus. Kohdassa ei kuitenkaan tyhjentävästi lueteltaisi toimivaltaisia viranomaisia.

Lisäksi kohdassa ulotettaisiin toimivaltaisen viranomaisen määritelmä koskemaan myös Puolustusvoimia, poliisia ja Rajavartiolaitosta näiden hoitaessa ehdotetussa 1 §:n 2 momentissa tarkoitettuja tehtäviä. Tältä osin kyse olisi puhtaasti kansallisesta sääntelystä.

Momentin 6 kohdassa määriteltäisiin *rekisterinpitäjä*. Määritelmä vastaisi pitkälti nykytilaa. Tarkentavasti kohdassa kuitenkin säädettäisiin, että rekisterinpitäjä olisi aina nimenomaan toimivaltainen viranomainen, joka yksin tai yhdessä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot tai jonka tehtäväksi rekisterinpito on lailla säädetty. Säännös mahdollistaisi siten niin sanotun yhteisrekisterinpitäjyyden nykytilaa vastaavasti.

Momentin 7 kohdassa määriteltäisiin *henkilötietojen käsittelijä*. Henkilötietojen käsittelijällä tarkoitettaisiin ehdotuksen mukaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Momentin 8 kohdan sisältämä määritelmä olisi uusi. Sen mukaan *vastaanottajalla* tarkoitettaisiin luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja. Vastaanottajalla ei ehdotetussa laissa kuitenkaan tarkoitettaisi sellaista toimivaltaista viranomaista, joka mahdollisesti saa henkilötietoja lain 1 §:n 1 momentin mukaisia tarkoituksia varten tietyn tutkinnan puitteissa.

Momentin 9 kohdassa määriteltäisiin *henkilötietojen tietoturvaloukkaus*. Nykylakiin ei sisälly vastaavaa määritelmää. Henkilötietojen tietoturvaloukkauksella tarkoitettaisiin kohdan mukaan tietoturvallisuutta koskevien säännösten rikkomista, josta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai oikeudeton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin. Määritelmänsä mukaan henkilötietojen tietoturvaloukkaus ei edellyttäisi sitä, että loukkauksesta on aiheutunut tosiasiallista vahinkoa rekisteröidylle.

Momentin 10 kohdassa määriteltäisiin, mitä tarkoitetaan ehdotetussa laissa mainituilla *asianmukaisilla suojoitoimenpiteillä*. Kohdan mukaan niillä tarkoitettaisiin sellaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan henkilötietojen käsittelyn lainmukaisuus, kun otetaan huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityjen oikeuksiin kohdistuvat riskit. Asianmukaisia suojoitoimenpiteitä ei ole mahdollista laissa tyhjentävästi määritellä, ja asianmukaisten suojoitoimenpiteiden luonne saattaa ajan kuluessa muun muassa teknologisen kehityksen vuoksi muuttua. Vastaavaa määritelmää ei nimenomaisesti sisälly rikosasioiden tietosuojadirektiiviin, mutta sitä ehdotetaan otettavan selkeyttävänä lakiin. Ehdotetussa laissa viitataan useissa kohdin asianmukaisiin suojoitoimenpiteisiin.

Momentin 11 kohdassa määriteltäisiin *geneettisiksi tiedoiksi* henkilötiedot, jotka koskevat sellaisia luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista selviää yksilöllistä tietoa kyseisen luonnollisen henkilön fysiologiasta tai terveydentilasta, ja jotka on saatu kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla tai muutoin. Määritelmä olisi uusi.

Momentin 12 kohdassa määriteltäisiin *biometriset tiedot*. Vastaavaa määritelmää ei sisälly nykyiseen lainsäädäntöön. Biometrisillä tiedoilla tarkoitettaisiin luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, joiden perusteella kyseinen luonnollinen henkilö

voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa. Biometrisiä tietoja olisivat esimerkiksi kasvokuvat ja sormenjälkitiedot.

Momentin 13 kohdan sisältämä *terveyttä koskevan tiedon* määritelmä olisi uusi. Sillä tarkoitettaisiin luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, jotka ilmaisevat hänen terveydentilansa. Määritelmän piiriin kuuluisivat myös esimerkiksi tieto terveystietojen tarjoamisesta. Rikosasioiden tietosuojadirektiivistä poiketen terveystietojen sijaan ehdotetaan käytettävän käsitettä *terveyttä koskeva tieto*.

Momentin 14 kohdassa määriteltäisiin *kolmas maa*. Sillä tarkoitettaisiin muuta maata kuin EU:n jäsenvaltiota, muuta Euroopan talousalueen maata tai Sveitsiä. Säännös ei aineellisesti muuttaisi nykytilaa, vaikka henkilötietolakiin ei ole sisällytynyt asiasta nimenomaista määritelmäsäännöstä.

Momentin 15 kohdassa määriteltäisiin, mitä ehdotetussa laissa tarkoitetaan *kansainvälisellä järjestöllä*. Käsitteellä tarkoitettaisiin järjestöä ja sen alaisia elimiä, joihin sovelletaan kansainvälistä julkisoikeutta, sekä muuta elintä, joka on perustettu kahden tai useamman maan välisellä sopimuksella tai tällaisen sopimuksen perusteella. Kohdassa tarkoitettu kansainvälinen järjestö olisi esimerkiksi Europol.

Pykälän 2 momentissa säädettäisiin, että mitä ehdotetussa laissa säädettäisiin toimivaltaisesta viranomaisesta, sovellettaisiin myös 1 momentin 5 kohdassa tarkoitettua tehtävää hoitamaan yksityiseen tahoon. Säännös olisi mahdollinen rikosasioiden tietosuojadirektiivin 3 artiklan 7 kohdan b alakohdan nojalla. Mainitun artiklan mukaan toimivaltaisella viranomaisella voitaisiin tarkoittaa myös kaikkia muita elimiä tai yksiköitä kuin viranomaisia, joille on jäsenvaltion lainsäädännössä annettu tehtäväksi käyttää julkista valtaa tai valtuuksia rikosten ennalta estämiseen, tutkimiseen, paljastamiseen tai rikoksiin liittyviin syyt toimiin tai rikosoikeudellisten seuraamusten täytäntöönpanoon. Suomessa lähtökohtaisesti vain viranomaiset hoitavat 1 momentin 5 kohdassa tarkoitettuja tehtäviä, mutta ehdotettu sääntely on tarpeen muissa EU-maissa tällaisia tehtäviä hoitavien yksityisten huomioon ottamiseksi.

Pykälän 3 momentin mukaan mitä ehdotetussa laissa säädettäisiin EU:n jäsenvaltiosta, sovellettaisiin myös muihin Euroopan talousalueeseen kuuluviin maihin ja Sveitsiin. Ehdotus perustuu direktiivin sääntelyyn. Euroopan talousalueeseen kuuluvat nykyisellään EU-maiden lisäksi Islanti, Liechtenstein ja Norja.

2 luku Henkilötietojen käsittelyn yleiset edellytykset

Luvussa säädettäisiin henkilötietojen käsittelyn yleisistä periaatteista, joita tulisi noudattaa aina käsiteltäessä henkilötietoja ehdotetun lain mukaisesti.

4 §. Laillisuusvaatimus. Pykälässä säädettäisiin henkilötietojen käsittelyn laillisuusvaatimuksesta. Ehdotettu pykälä perustuu rikosasioiden tietosuojadirektiivin 4 artiklan 1 kohdan a ja b alakohtaan sekä 8 artiklan 1 momenttiin. Pykälä vastaisi pääpiirteissään henkilötietolain 5 §:ää, jossa säädetään huolellisuusvelvoitteesta. Viimeksi mainitun lainkohdan mukaan henkilötietoja tulee käsitellä laillisesti, minkä lisäksi käsittelyssä tulee noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta.

Ehdotetun pykälän *1 momentin* mukaan henkilötietoja saa käsitellä ainoastaan, mikäli käsittelystä säädetään laissa. Lailla tarkoitetaan tässä yhteydessä sekä kotoperäistä että EU-lainsäädäntöä. Lisäksi momentissa edellytettäisiin, että käsittely on tarpeen toimivaltaisen viranomaisen 1 §:ssä tarkoitetun tehtävän suorittamiseksi. Tarpeellisuusvaatimuksen mukaisesti henkilötietoja tulisi käsitellä siten vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.

Pykälän *2 momentissa* säädettäisiin, että henkilötietoja on käsiteltävä asianmukaisesti ja huolellisesti. Näistä vaatimuksista seuraisi myös velvollisuus käsitellä henkilötietoja hyvän tietojenkäsittelytavan mukaisesti.

5 §. Käyttötarkoitussidonnaisuus. Pykälässä säädettäisiin käyttötarkoitussidonnaisuuden periaatteesta. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 4 artiklan 1 kohdan b alakohta, 2 ja 3 kohta sekä 9 artikla. Henkilötietolain 7 §:äänkin on sisältynyt käyttötarkoitussidonnaisuutta koskeva säännös.

Ehdotetun pykälän *1 momentin* mukaan henkilötietoja saa kerätä vain tiettyjä nimenomaisia tarkoituksia varten, eikä niitä saa myöhemmin käsitellä kyseisten tarkoitusten kanssa yhteensopimattomalla tavalla.

Pykälän *2 momentin* mukaan ehdotetun lain 1 §:ssä säädettyä tarkoitusta varten kerättyjä henkilötietoja saa käsitellä muuhun kuin 1 §:ssä säädettyyn tarkoitukseen vain, jos tällaisesta käsittelystä säädetään laissa. Lakisääteisyysvaatimus voisi tulla täytetyksi niin kansallisella kuin unioninkin lainsäädännöllä. Tällaisen lain olisi täytettävä rikosasioiden tietosuojadirektiivin vaatimukset käsittelyn tarpeellisuuden ja oikeasuhtaisuuden osalta siten kuin rikosasioiden tietosuojadirektiivin 4 artiklan 2 kohdan b

alakohdassa edellytetään. Jos henkilötietoja käsitellään säännöksessä viitattuihin muihin tarkoituksiin, sovellettaisiin lähtökohtaisesti yleistä tietosuojasetusta.

Pykälän 3 *momentissa* säädettäisiin, että sama tai toinen rekisterinpitäjä saa käsitellä henkilötietoja myös yleisen edun mukaista arkistointia taikka tieteellistä, tilastollista tai historiallista käsittelyä varten 1 §:ssä säädettyjä tarkoituksia varten. Edellytyksenä tällöin kuitenkin olisi, että rekisteröidyn oikeuksia koskevat asianmukaiset suojatoimet on toteutettu. Siltä osin kun pykälässä tarkoitettu käsittely tapahtuu muihin kuin ehdotetun lain 1 §:n mukaisiin tarkoituksiin, käsittelyyn sovellettaisiin yleistä tietosuojasetusta, ehdotettua tietosuojalakia sekä mahdollista henkilötietojen käsittelyä koskevaa erityislainsäädäntöä.

Rekisterinpitäjän tulisi kyetä osoittamaan, että se on noudattanut ehdotetun pykälän säännöksiä.

6 §. Tarpeellisuusvaatimus. Ehdotetulla pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 4 artiklan 1 kohdan c ja e alakohta sekä 5 artikla. Pykälässä säädettäisiin tarpeellisuusvaatimuksesta ja siihen olennaisesti liittyvästä säilytyksen rajoituksista. Yhdessä säännökset toteuttaisivat tietojen minimoinnin periaatetta. Tarpeellisuusvaatimuksesta säädetään nykyisin henkilötietolain 9 §:n 1 *momentissa*.

Pykälän 1 *momentin* mukaan käsiteltävien henkilötietojen tulisi olla käsittelyn tarkoituksen kannalta asianmukaisia ja tarpeellisia, eivätkä ne saisi olla liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään. Tarpeettomat henkilötiedot olisi niin ikään poistettava ilman aiheetonta viivytystä. Rekisterinpitäjän olisi tarvittaessa kyettävä osoittamaan henkilötietojen käsittelyn tarpeellisuus.

Pykälän 2 *momentin* mukaan henkilötiedot saisi säilyttää muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan kuin on tarpeellista henkilötietojen käsittelyn tarkoituksen kannalta.

Rikosasioiden tietosuojadirektiivin 5 artiklan mukaan jäsenvaltioiden on säädettävä siitä, että henkilötietojen poistamista tai niiden säilyttämisen tarpeellisuuden säännöllistä tarkistamista varten vahvistetaan asianmukaiset määräajat. Henkilötietojen säilyttämisen tarpeellisuutta olisi pykälän 3 *momentin* mukaan arvioitava vähintään viiden vuoden välein, jollei henkilötietojen säilytysajoista muualla toisin säädettäisi. Pykälällä varmistettaisiin, että henkilötietojen säilyttämisen tarpeellisuus arvioidaan säännöllisesti myös siinä tapauksessa, ettei erityislainsäädännössä ole erityisiä säännöksiä tietojen säilytysajoista tai säilytyksen tarpeellisuuden arvioimisesta.

7 §. Virheettömyysvaatimus. Pykälässä säädettäisiin virheettömyysvaatimuksesta, joka on yksi henkilötietojen käsittelyä koskevista periaatteista. Pykälällä täytettäisiin rikosasioiden tietosuojadirektiivin 4 artiklan 1 kohdan d alakohdan sisältämä lainsäädäntötoimeksianto. Henkilötietolain 9 §:n 2 momentti sisältää säännöksen virheettömyysvaatimuksesta. Vaikka vaatimuksen perustavanlaatuinen lähtökohta säilyisi ennallaan, tarkistettaisiin säännöksen sanamuotoa henkilötietolakiin nähden vastamaan paremmin rikosasioiden tietosuojadirektiiviä.

Pykälän mukaan käsiteltävien henkilötietojen tulisi olla virheettömiä ja käsittelyn tarkoitus huomioon ottaen päivitettyjä. Vaatimus tarkoittaisi käytännössä esimerkiksi sitä, että rekisterinpitäjän tulee toteuttaa kaikki kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden virheelliset tiedot poistetaan tai oikaistaan viipymättä. Toimivaltaisten viranomaisten olisi niin ikään varmistettava, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja siirretä tai aseteta saataville tai ylipäättään kerätä. Pykälässä tarkoitetun päivittämisvelvoitteen merkitystä arvioitaessa olisi otettava huomioon henkilötietojen käsittelyn tarkoitus sekä käsittelyn merkitys rekisteröidyn yksityisyyden suojalle ja oikeusturvalle.

8 §. Eräiden henkilötietojen erottaminen toisistaan. Pykälässä säädettäisiin velvollisuudesta erottaa eräät henkilötiedot toisistaan. Pykälä perustuu rikosasioiden tietosuojadirektiivin 6 artiklaan sekä 7 artiklan 1 kohtaan. Vastaavaa säännöstä ei sisälly henkilötietolakiin. Ehdotetulla säännöksellä on kuitenkin tiivis yhteys esimerkiksi ehdotetun lain 7 §:ssä säädettyyn virheettömyysvaatimukseen.

Pykälän 1 momentissa säädettäisiin, että rekisterinpitäjän on erotettava tarvittaessa ja mahdollisuuksien mukaan selvästi toisistaan henkilötiedot, jotka koskevat käsiteltävän asian kannalta eri asemassa olevia rekisteröityjä. Erottamisen toteuttamiseksi tulisi toteuttaa kaikki kohtuulliset toimenpiteet, kun otetaan huomioon tietojen erillään pidon merkitys.

Eri asemassa toisiinsa nähden voitaisiin katsoa olevan esimerkiksi henkilöt, joiden on syytä epäillä syyllistyneen tai olevan syyllistymässä rikokseen sekä henkilöt, jotka on tuomittu rikoksesta. Erillään olisi pidettävä henkilötiedot, jotka koskevat rikokseen nähden kolmansia osapuolia, kuten henkilöitä, joita voidaan kutsua todistamaan rikokseen liittyvän tutkinnan yhteydessä tai sitä seuraavassa rikosoikeudellisessa menettelyssä taikka henkilöitä, jotka voivat antaa tietoa rikoksesta.

Pykälän 2 momentissa säädettäisiin, että tosiseikkoihin perustuvien henkilötietojen erottamiseksi henkilökohtaisiin arvioihin perustuvista henkilötiedoista olisi toteutettava kaikki kohtuulliset toimenpiteet. Esimerkiksi oikeudellisissa menettelyissä saadaan usein lausuntoja, jotka sisältävät henkilötietoja, mutta jotka perustuvat luonnollisten henkilöiden subjektiiviseen havaintoon. Tällaiset tiedot eivät aina ole todennettavissa,

jolloin ne tulisi lähtökohtaisesti pitää erillään tosiseikkoihin perustuvista henkilötiedoista.

9 §. *Siirrettävien tai saataville asetettavien henkilötietojen laadun varmentaminen.* Pykälässä asetettaisiin vaatimukset siirrettävien tai saataville asetettavien henkilötietojen laadun varmentamiselle. Siirtämisellä voidaan tarkoittaa sekä henkilötietojen teknistä siirtämistä että henkilötietojen varsinaista luovuttamista. Pykälässä asetettaisiin korostettu huolellisuus- ja virheettömyysvaatimus henkilötietojen siirtämiselle ja saataville asettamiselle. Säännöksellä pyritäisiin varmistumaan, että siirrettävät ja saataville asetettavat tiedot olisivat mahdollisimman laadukkaita. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 7 artiklan 2 ja 3 kohta.

Pykälän 1 *momentin* mukaan toimivaltaisen viranomaisen olisi toteutettava kaikki kohdulliset toimenpiteet sen varmistamiseksi, ettei virheellisiä, epätäydellisiä taikka vanhentuneita henkilötietoja siirretä eikä aseteta saataville. Tätä varten kunkin toimivaltaisen viranomaisen olisi varmennettava mahdollisuuksien mukaan henkilötietojen laatu aina ennen niiden siirtämistä tai saataville asettamista.

Pykälän 2 *momentissa* säädettäisiin, että kaikkiin henkilötietojen siirtoihin olisi mahdollisuuksien mukaan lisättävä sellaiset tarvittavat tiedot, joiden avulla vastaanottava toimivaltainen viranomainen voisi arvioida henkilötietojen paikkansapitävyyttä, täydellisyyttä, luotettavuutta sekä sitä, miltä osin tiedot ovat ajantasaisia.

Jos ilmenee, että virheellisiä henkilötietoja on siirretty tai että henkilötietoja on siirretty lainvastaisesti, olisi asiasta pykälän 3 *momentissa* ehdotetun mukaisesti ilmoitettava viipymättä vastaanottajalle. Vastaanottajan olisi tällöin asiasta tiedon saatuaan oikaistava tai poistettava saamansa henkilötiedot tai rajoitettava niiden käsittelyä. Myös henkilötiedot siirtäneen toimivaltaisen viranomaisen olisi luonnollisesti toteutettava asianmukaiset toimenpiteet, kuten korjattava sillä olevat virheelliset henkilötiedot.

10 §. *Ilmoittamisvelvollisuus käsittelyn erityisistä edellytyksistä.* Pykälässä säädettäisiin toimivaltaisen viranomaisen ilmoittamisvelvollisuudesta käsittelyn erityisiä edellytyksiä koskien rikosasioiden tietosuojadirektiivin 9 artiklan 3 ja 4 kohdan mukaisesti.

Pykälän 1 *momentin* mukaan mikäli henkilötietojen käsittelyyn liittyy laissa säädettyjä erityisiä edellytyksiä, toimivaltaisen viranomaisen on henkilötietojen luovutuksen tai siirron yhteydessä ilmoitettava henkilötietojen vastaanottajalle kyseisistä edellytyksistä sekä velvollisuudesta noudattaa niitä. Tällaisiin edellytyksiin voisi kuulua esimerkiksi kielto siirtää henkilötietoja edelleen tai käyttää henkilötietoja muissa kuin siinä tarkoituksessa, jota varten tiedot on toimitettu vastaanottajalle. Erityisiin edellytyksiin voisi kuulua myös kielto ilmoittaa rekisteröidylle tiedonsaantioikeuden rajoittamisesta

ilman tietoja siirtävän toimivaltaisen viranomaisen etukäteen antamaa hyväksyntää. Tällaisista erityisistä edellytyksistä voitaisiin säätää toimivaltaisiin viranomaisiin sovellettavassa erityislainsäädännössä.

Pykälän 2 *momentissa* ehdotetaan säädettävän, että toimivaltainen viranomainen ei saa asettaa henkilötietojen käsittelylle tiukempia edellytyksiä kuin mitä sovelletaan kansallisesti samankaltaisiin tiedonsiirtoihin silloin, kun se siirtää henkilötietoja Euroopan unionissa sijaitsevalle vastaanottajalle.

11 §. *Erityisiä henkilötietoryhmiä koskeva käsittely.* Pykälässä säädettäisiin erityisistä henkilötietoryhmistä ja niitä koskevasta käsittelystä. Säännös perustuisi rikosasioiden tietosuojadirektiivin 10 artiklaan.

Erityisiin henkilötietoryhmiin kuuluvista tiedoista säädettäisiin pykälän 1 *momentissa*. Henkilötietolakia vastaavalla tavalla erityisiin henkilötietoryhmiin kuuluvista tiedoista käytettäisiin myös nimitystä arkaluonteiset henkilötiedot. Tällaisia tietoja olisivat henkilötiedot, joista ilmenee etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus taikka ammattiliiton jäsenyys. Niin ikään arkaluonteisia henkilötietoja olisivat geneettiset tiedot, luonnollisen henkilön yksiselitteiseen tunnistamiseen tarkoitettut biometriset tiedot, kuten sormenjälkitiedot ja kasvokuvat, tai terveyttä taikka luonnollisen henkilön seksuaalista käyttäytymistä ja seksuaalista suuntautumista koskevat tiedot.

Henkilötietolain 11 §:n 3 kohdasta poikkeavasti arkaluonteisina henkilötietoina ei pidettäisi tietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta. Viimeksi mainittujen henkilötietojen käsittely kuitenkin aina edellyttää, että käsittelystä on säädetty laissa.

Nykytilaa vastaavasti arkaluonteisten henkilötietojen käsittely olisi lähtökohtaisesti kielletty. Arkaluonteisten henkilötietojen käsittely olisi sallittu vain pykälän 2 *momentissa* luetelluissa tilanteissa. Käsittely olisi ehdotetun säännöksen mukaan sallittu, jos se on välttämätöntä ja edellyttäen, että rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu. Lisäksi edellytyksenä olisi, että käsittelystä säädetään laissa, että käsittely koskee tietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi taikka että rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen sitä edellyttää.

12 §. *Henkilötunnuksen käsittely.* Pykälässä säädettäisiin henkilötunnuksen käsittelystä. Rikosasioiden tietosuojadirektiiviin ei sisälly nimenomaista henkilötunnuksen käsittelyä koskevaa sääntelyä. Ehdotettu sääntely olisi siten puhtaasti kansallista. Henkilötunnuksen käsittelyä koskeva säännös sisältyy myös henkilötietolain 13 §:ään. Vaikka

henkilötunnusta ei pidetäkään arkaluonteisena henkilötietona, on sen erityispiirteiden vuoksi käsittelystä syytä edelleenkin säätää laissa.

Henkilötunnuksen käsittelyn erityisistä edellytyksistä säädettäisiin pykälän *1 momentissa*. Ehdotetun säännöksen mukaan henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää toimivaltaisen viranomaisen laissa säädetyn tehtävän suorittamiseksi taikka rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi. Lisäksi käsittely olisi sallittua, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää ehdotetun lain 5 §:n 3 momentin mukaista historiallista tai tieteellistä tutkimusta taikka tilastointia varten.

Ehdotetun *2 momentin* mukaan henkilötunnusta ei saa tarpeettomasti merkitä henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin. Ehdotus vastaa nykytilaa.

13 §. Automatisoidut yksittäispäätökset. Pykälässä säädettäisiin automatisoiduista yksittäispäätöksistä, joita koskeva säännös sisältyy rikosasioiden tietosuojadirektiivin 11 artiklaan. Henkilötietolain 31 §:ään sisältyy automatisoituja päätöksiä koskeva, hieman erisältöinen säännös.

Ehdotetun pykälän mukaan sellaisen päätöksen tekeminen, joka perustuu pelkästään automatisoituun henkilötietojen käsittelyyn ja jolla on rekisteröityä koskevia kielteisiä oikeusvaikutuksia tai joka muutoin on hänen kannaltaan merkittävä, on kielletty. Tällaisen automatisoidun yksittäispäätöksen tekeminen olisi ehdotetun säännöksen mukaan sallittua ainoastaan, jos muualla laissa toisin säädetään.

Käytännössä tällaisesta automatisoidusta päätöksenteosta tulisi siten säätää aina erityislainsäädännössä. Tällaisen sääntelyn tulisi täyttää rikosasioiden tietosuojadirektiivin vaatimukset. Näitä ovat esimerkiksi vaatimus siitä, että rekisteröidyllä on oikeus vaatia, että käsittelyyn osallistuu rekisterinpitäjän toimesta luonnollinen henkilö. Automatisoidusta päätöksenteosta säädettäessä tulisi myös toteuttaa tarvittavat toimenpiteet rekisteröidyn oikeuksien turvaamiseksi. Tällaisiin asianmukaisiin suojatoimiin voisi kuulua esimerkiksi tällaisesta käsittelystä ilmoittaminen rekisteröidylle, jotta rekisteröity voisi esittää asiassa oman kantansa, saada selvityksen kyseisen arvioinnin jälkeen tehdystä päätöksestä taikka vastustaa tällaista päätöstä tai riitauttaa sen. Erityisen tärkeää tarvittavista asianmukaisista toimenpiteistä varmistuminen olisi silloin, jos automatisoitu päätös perustuu ehdotetussa 11 §:ssä säädettyihin arkaluonteisiin henkilötietoihin. Mahdollinen profilointi ei myöskään saa johtaa syrjintään.

3 luku Rekisterinpitäjä ja henkilötietojen käsittelijä

14 §. Rekisterinpitäjän vastuu. Pykälässä säädettäisiin ehdotetussa laissa tarkoitetun rekisterinpitäjän vastuusta. Säännös perustuisi rikosasioiden tietosuojadirektiivin 19 artiklan 1 momenttiin.

Pykälän 1 momentissa säädettäisiin siitä, että rekisterinpitäjä on henkilötietolain sääntelyä vastaavasti vastuussa siitä, että henkilötietoja käsitellään lainmukaisesti.

Pykälän 2 momentissa asetettaisiin rekisterinpitäjälle velvollisuus toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla se voi varmistaa ja myös osoittaa, että henkilötietojen käsittely on lainmukaista. Toimenpiteiden toteuttamisessa olisi ehdotetun säännöksen mukaan otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin kohdistuvat riskit. Momentissa tarkoitettuihin rekisterinpitäjän toimenpiteisiin tulisi sisältyä myös heikommassa asemassa olevien luonnollisten henkilöiden, kuten lasten ja ihmiskaupan uhrien, henkilötietojen käsittelyä koskevien erityisten suojatoimien laatiminen ja täytäntöönpano.

Pykälässä korostuisi huolellisuus- ja laillisuusvaatimuksen lisäksi niin sanottu rekisterinpitäjän osoittamisvelvollisuus. Rekisterinpitäjän olisi säännöksen mukaisesti kyettävä osoittamaan myös esimerkiksi jälkikäteen, että henkilötietojen käsittely on lainmukaista.

15 §. Sisäänrakennettu ja oletusarvoinen tietosuoja. Pykälässä säädettäisiin sisäänrakennetusta ja oletusarvoisesta tietosuojasta (*privacy by design ja privacy by default*) ja sillä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 20 artikla. Kyseessä olisi nykytilaan nähden uudenkaltainen velvoite.

Pykälän 1 momentin mukaan rekisterinpitäjän tulisi jo henkilötietojen käsittelytapoja määrittäessään sekä itse henkilötietojen käsittelyn yhteydessä toteuttaa asianmukaiset tekniset ja organisatoriset suojatoimenpiteet varmistaakseen käsittelyn lainmukaisuuden ja rekisteröidyn oikeuksien suojaamisen. Toimenpiteiden toteuttamisessa olisi huomioitava käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset samoin kuin ne riskit, jotka käsittely henkilön oikeuksille aiheuttaa. Momentissa tarkoitettuihin toimenpiteisiin voisi kuulua esimerkiksi pseudonymisoinnin käyttö niin pian kuin se on käsittelyn tarkoituksen kannalta mahdollista.

Riskin todennäköisyys ja vakavuus olisi määriteltävä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten mukaan. Riski tulisi arvioida objektiivisen arvion perusteella. Korkean riskin voitaisiin katsoa olevan kyseessä etenkin silloin, kun käsillä on

rekisteröityjen oikeuksia ja vapauksia heikentävä riski. Esimerkiksi arkaluonteisten henkilötietoryhmien tai erityisen haavoittuvien henkilöryhmien tietojen käsittely asettaa usein suuremman riskin henkilön oikeuksille, jolloin toimenpiteiden toteuttamiselle olisi syytä usein asettaa korkeammat vaatimukset. Toisaalta käsittelytyyppeinä tietojen luovuttaminen tai saataville asettaminen voivat olla myös erityisen riskipitoisia.

Pykälän 2 *momentissa* edellytettäisiin, että rekisterinpitäjä toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen, että oletusarvoisesti käsitellään vain kunkin erityisen käsittelytarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskisi niin kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa kuin saatavilla oloakin. Asianmukaisilla toimenpiteillä olisi erityisesti varmistettava, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman luonnollisten henkilöiden piirin saataville ilman asianomaisen henkilön myötävaikutusta.

16 §. Yhteiset rekisterinpitäjät. Pykälässä säädettäisiin erityisistä vaatimuksista tilanteissa, joissa on käsillä niin sanottu yhteisrekisterinpitäjäyys. Säännös perustuisi rikosasioiden tietosuojadirektiivin 21 artiklaan. Henkilötietolakikin mahdollistaa, että rekisterinpitäjiä on useampi, mutta se ei kuitenkaan sisällä ehdotetun pykälän kaltaista säännöstä, jolla täsmennetään yhteisten rekisterinpitäjien keskinäisiä suhteita.

Pykälän 1 *momentissa* säädettäisiin, että jos kaksi tai useampi rekisterinpitäjä määrittää yhdessä käsittelyn tarkoitukset ja keinot, niiden tulisi sopia keskinäisestä vastuunjaostaan ehdotetun lain mukaisten velvollisuuksien hoitamisessa, jollei vastuunjaosta ole säädetty laissa. Keskinäisessä vastuunjaon määrittämisessä tulisi huolellisesti varmistaa, että lain vaatimukset tulevat kaikilta osin huomioituksi. Vaikka tärkeimmistä vastuunjako- ja velvollisuuksiin liittyvistä tehtävistä säädetään vastaisuudessaakin pitkälti laissa, antaisi ehdotettu säännös joustavuutta rekisterinpitäjien välisen tehtävänjaon suhteen.

Pykälän 2 *momentissa* säädettäisiin, että 1 momentissa tarkoitettujen rekisterinpitäjien on nimettävä keskuudestaan yhteyspisteenä toimiva rekisterinpitäjä. Yhteyspisteenä toimiva rekisterinpitäjä olisi se, johon rekisteröity voisi ensisijaisesti olla yhteydessä oikeuksiensa käyttöä koskevissa asioissa. Momentissa kuitenkin säädettäisiin, että rekisteröity voi kuitenkin aina käyttää ehdotetun lain mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään.

17 §. Henkilötietojen käsittelijä. Pykälässä säädettäisiin henkilötietojen käsittelijästä rikosasioiden tietosuojadirektiivin 22 artiklan 1–4 kohdan edellyttämällä tavalla.

Pykälän 1 *momentin* mukaan henkilötietoja rekisterinpitäjän lukuun käsittelevän olisi annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä muutoinkin

riittävät takeet niistä organisatorisista ja teknisistä toimenpiteistä, joilla se varmistaa, että henkilötietoja käsitellään ehdotetussa laissa säädettyjen vaatimusten mukaisesti. Vastaavankaltainen säännös sisältyy henkilötietolain 32 §:n 2 momenttiin. Ehdotetun säännöksen perusteella myös henkilötietojen käsittelijän olisi otettava huomioon esimerkiksi sisäänrakennetun ja oletusarvoisen tietosuojan periaate.

Pykälän 2 momentissa asetettaisiin kieltö henkilötietojen käsittelijälle käsitellä henkilötietoja muutoin kuin rekisterinpitäjän ohjeiden mukaisesti. Jos henkilötietojen käsittelijä määritteli ehdotetun lain vastaisesti käsittelyn tarkoitukset ja keinot, katsottaisiin käsittelijä rekisterinpitäjäksi kyseisen lainvastaisen käsittelyn osalta. Henkilötietojen käsittelijä ei ehdotetun säännöksen mukaan myöskään saa siirtää henkilötietojen käsittelyä toiselle käsittelijälle ilman rekisterinpitäjän kirjallista lupaa. Tällainen rekisterinpitäjän suostumus voisi olla joko tapauskohtainen tai yleinen. Jos rekisterinpitäjä antaisi siirtoon yleisen suostumuksen, henkilötietojen käsittelijän olisi kuitenkin ilmoitettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden käsittelijöiden lisäämistä tai vaihtamista. Rekisterinpitäjällä olisi myös oikeus kieltää tällaiset muutokset.

Henkilötietojen käsittelijän suorittamasta henkilötietojen käsittelystä olisi pykälän 3 momentin mukaan tehtävä kirjallinen sopimus tai annettava kirjallinen määräys. Sopimus tai määräys voisi olla myös sähköisessä muodossa. Asiakirjasta tulisi ilmetä käsiteltävät henkilötiedot, käsittelyn kesto, luonne ja tarkoitus, käsiteltävät henkilötietoryhmät ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.

Ehdotetussa 3 momentissa tarkoitetussa asiakirjassa olisi lisäksi nimenomaisesti määrättävä, että henkilötietojen käsittelijä toimii ainoastaan rekisterinpitäjän ohjeiden mukaisesti. Lisäksi edellytettäisiin määrättävän tai sovittavan siitä, että henkilötietojen käsittelijä varmistaa, että henkilötietoja käsittelevät luonnolliset henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai että heitä sitoo lakisääteinen salassapitovelvollisuus. Henkilötietojen käsittelijän tulee avustaa rekisterinpitäjää kaikin tarkoituksenmukaisin tavoin, jotta voidaan varmistaa, että rekisteröidyn oikeuksia koskevia säännöksiä noudatetaan.

Lisäksi asiakirjasta tulisi ilmetä, että henkilötietojen käsittelijä rekisterinpitäjän valinnan mukaan poistaa taikka palauttaa tietojenkäsittelypalveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, jollei laissa edellytetä henkilötietojen säilyttämistä. Asiakirjassa olisi myös oltava maininta siitä, että käsittelijä saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen ehdotetun pykälän noudattamisen osoittamiseksi sekä täyttää ehdotetussa pykälässä tarkoitetut toisen käsittelijän käyttöä koskevat edellytykset.

18 §. Seloste käsittelytoimista. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 24 artiklaan ja siinä asetettaisiin velvollisuus sekä rekisterinpitäjälle että henkilötietojen käsittelijälle laatia seloste henkilötietojen käsittelytoimista. Pykälässä tarkoitettujen selosteiden tulisi olla kirjallisia, ja ne voisivat olla myös sähköisessä muodossa. Rekisterinpitäjän ja henkilötietojen käsittelijän olisi pyydettäessä esitettävä saatavilla olevat selosteet valvontaviranomaiselle. Ehdotettu säännös eroaisikin henkilötietolain 10 §:n mukaisesta rekisteriselosteesta, sillä ehdotetussa pykälässä säädettyä selostetta ei tarvitsisi pitää yleisesti saatavilla.

Pykälän 1 momentissa säädettäisiin rekisterinpitäjän käsittelytoimia koskevasta selosteesta. Säännöksen mukaan rekisterinpitäjän olisi ylläpidettävä sen vastuulle kuuluvasta henkilötietojen käsittelystä kirjallista selostetta, johon sisältyy vähintään momentissa luetellut tiedot. Pakollisten tietojen lisäksi rekisteriselosteessa voisi toisinaan olla syytä kertoa muitakin informaation kannalta tärkeitä asioita. Pakollisten tietojen joukko olisi laajempi kuin mitä henkilötietolain 10 §:ssä edellytetään. Uusia vaatimuksia olisivat esimerkiksi sen kirjaaminen, käytetäänkö profilointia sekä eri henkilötietoryhmien poistamisen suunnitellut määräajat. Jos henkilötietoja siirretään kolmanteen maahan tai kansainväliselle järjestölle, tulisi selosteesta käydä ilmi, mikä kolmas maa tai kansainvälinen järjestö on kyseessä.

Momentissa mainitulla profiloinnilla tarkoitettaisiin mitä tahansa henkilötietojen automaattista käsittelyä, jolla analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin tai jolla muutoin henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia. Profiloinnin määritelmä sisältyy direktiivin 3 artiklan 4 alakohtaan.

Pykälän 2 momentissa edellytettäisiin, että myös henkilötietojen käsittelijä ylläpitää kirjallista selostetta kaikesta rekisterinpitäjän lukuun suoritettavasta henkilötietojen käsittelystä. Vastaavaa velvollisuutta ei sisälly voimassa olevaan henkilötietolakiin. Käsittelijän ylläpitämän selosteen tulisi sisältää tiedot ensinnäkin henkilötietojen käsittelijästä ja tietosuojavastaavasta sekä näiden yhteystiedoista. Lisäksi selosteessa tulisi ilmoittaa kaikki ne rekisterinpitäjät, joiden lukuun käsittelijä toimii sekä näiden nimet ja yhteystiedot, sekä kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät. Lisäksi jos rekisterinpitäjä on nimenomaisesti niin ohjeistanut, tulisi selosteessa ilmoittaa mahdolliset tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle. Mahdollisuuksien mukaan selosteeseen tulisi myös sisällyttää yleinen kuvaus ehdotetun lain 31 §:ssä tarkoitetuista teknisistä ja organisatorisista turvatoimista.

19 §. Lokitiedot. Pykälässä säädettäisiin velvollisuudesta kerätä ja säilyttää lokitietoja. Pykälällä täytettäisiin rikosasioiden tietosuojadirektiivin 25 artiklaan sisältyvä lainsäädäntötoimeksianto. Vastaavaa lokitusvelvollisuutta ei sisälly henkilötietolakiin, mutta erityislainsäädäntöön, kuten henkilötietojen käsittelystä poliisitoimessa annettuun lakiin, velvollisuus on nykyisinkin sisältynyt.

Myös lokitietoja on pidettävä henkilötietoina. Ne ovat niitä henkilöitä koskevia henkilötietoja, jotka käyttävät tietojärjestelmiä. Koska muut henkilöt eivät ole tässä tarkoitettuja rekisteröityjä, ei heillä olisi tarkastusoikeutta pykälässä tarkoitettuihin lokitietoihin. Mahdollisuus saada tietoja viranomaisen lokeista voi kuitenkin tulla kyseeseen, jos henkilöllä on oikeus saada kyseisiä tietoja lokeista julkisuuslain 11 §:n nojalla, sillä puheena olevia lokeja on pidettävä viranomaisten asiakirjoina.

Pykälän 1 momentissa säädettäisiin, että rekisterinpitäjän ja henkilötietojen käsittelijän on säilytettävä lokitiedot automaattisessa tietojenkäsittelyjärjestelmässään suoritetusta henkilötietojen keräämisestä, muuttamisesta, kyselystä, luovuttamisesta, siirtämisestä, yhdistämisestä ja poistamisesta. Lisäksi edellytettäisiin, että kyselyjä ja luovutuksia koskevien lokitietojen avulla on voitava selvittää kyselyn ja luovutuksen peruste, toteutuspäivä ja -aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys.

Pykälän 2 momentissa säädettäisiin niistä tarkoituksista, joihin lokitietoja saisi käyttää. Säännökseen sisältyvä luettelo olisi tyhjentävä. Lokitietoja saisi käyttää ainoastaan käsittelyn lainmukaisuuden tarkistamiseen, henkilötietojen eheyden ja turvallisuuden varmistamiseen, rikosoikeudellisiin menettelyihin sekä sisäiseen valvontaan. Sisäiseen valvontaan voisivat kuulua myös toimivaltaisten viranomaisten sisäiset kurinpitomenettelyt.

20 §. Tietosuojaa koskeva vaikutustenarviointi. Pykälässä säädettäisiin rekisterinpitäjän velvollisuudesta tehdä tietosuojaa koskeva vaikutustenarviointi. Vastaavaa säännöstä ei sisälly henkilötietolakiin. Säännöksellä on kuitenkin kiinteä yhteys henkilötietojen käsittelyn yleisiin periaatteisiin. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 27 artikla.

Pykälän 1 momentin mukaan rekisterinpitäjän tulisi ennen henkilötietojen käsittelyyn ryhtymistä arvioida suunnittelemiensa käsittelytoimien vaikutukset henkilötietojen suojaan. Velvollisuus olisi yleinen ja tulisi kyseeseen esimerkiksi aina, kun rekisterinpitäjän on tarkoitus ryhtyä jollakin tavalla uudenlaiseen henkilötietojen käsittelyyn tai jos henkilötietojen käsittelyssä tapahtuu muutoksia.

Mikäli rekisterinpitäjän suunnittelema henkilötietojen käsittely vaikuttaisi 1 momentin mukaisesti tehtävän arvion mukaan merkittävän riskin luonnollisen henkilön oikeuksien toteutumiselle, rekisterinpitäjän olisi pykälän 2 *momentin* mukaisesti tehtävä kirjallinen vaikutustenarviointi. Merkittävä riski voisi tulla kyseeseen esimerkiksi silloin, kun henkilötietojen käsittelyä ulkoistetaan, kun henkilötietoja siirretään kolmansiin maihin tai kun tehdään tietojärjestelmiin kohdistuvia uudistuksia.

Vaikutustenarviointiin olisi ehdotetun säännöksen mukaan sisällytettävä yleinen kuvaus suunnitelluista käsittelytoimista, arvio rekisteröidyn oikeuksiin kohdistuvista riskeistä ja toimet niiden vähentämiseksi sekä toimet, joilla henkilötietojen suoja ja lain noudattaminen varmistetaan. Arviossa olisi otettava huomioon etenkin suunnitellun käsittelyn luonne, laajuus, asiayhteys ja tarkoitus. Momentissa tarkoitettu vaikutustenarviointi olisi siten yksityiskohtaisempi kuin 1 momentissa tarkoitettu ensivaiheen vaikutustenarviointi. Vaikutustenarviointi olisi kohdistettava esimerkiksi asianomaisiin käsittelytoimien järjestelmiin ja prosesseihin, eikä yksittäisiin tapauksiin.

21 §. *Valvontaviranomaisen ennakkuuleminen.* Pykälässä säädettäisiin velvollisuudesta kuulla Tietosuojavirastoa ennakolta ja se perustuisi rikosasioiden tietosuojadirektiivin 28 artiklan 1, 3, 4 ja 5 kohtaan.

Pykälän 1 *momentin* mukaan rekisterinpitäjän tai henkilötietojen käsittelijän olisi eräissä tilanteissa kuultava Tietosuojavirastoa ennen henkilötietojen käsittelyn aloittamista. Velvollisuus Tietosuojaviraston ennakkuulemiseen olisi ensinnäkin silloin, kun edellä ehdotetun 20 §:n 2 momentissa tarkoitettu kirjallinen vaikutustenarviointi osoittaisi, että suunnitelluista suojatoimenpiteistä huolimatta käsittely aiheuttaa merkittävän jäännösriskin rekisteröidyn oikeuksille. Lisäksi ennakkuulemisvelvollisuus aktualisoituisi silloin, kun henkilötietojen käsittely muutoin ja erityisesti uusien tekniikoiden, mekanismien tai menettelyjen käyttämisen johdosta aiheuttaisi merkittävän riskin rekisteröityjen oikeuksien kannalta.

Pykälän 2 *momentissa* säädettäisiin, että Tietosuojavirasto voisi laatia luettelon 1 momentissa tarkoitetuista ennakkuulemistä edellyttävistä käsittelytoimenpiteistä.

Pykälän 3 *momentissa* asetettaisiin rekisterinpitäjälle velvollisuus toimittaa Tietosuojavirastolle kirjallinen vaikutustenarviointi ja pyynnöstä kaikki muut sellaiset tiedot, joiden avulla virasto voisi arvioida henkilötietojen käsittelyn lainmukaisuutta.

Pykälän 4 *momentissa* säädettäisiin tilanteista, joissa Tietosuojavirasto katsoo, että 1 momentissa tarkoitettu käsittely muodostuisi ehdotetun lain vastaiseksi. Tällöin Tietosuojaviraston tulisi kuuden viikon kuluessa kuulemispyynnön vastaanottamisesta antaa rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle ohjausta käsittelyn

saattamiseksi lainmukaiseksi. Ohjauksella tarkoitettaisiin yleistä ohjeiden ja neuvonnan antamista. Määräaika voitaisiin jatkaa kuukaudella, jos suunnitellun käsittelyn monimutkaisuus sitä edellyttää. Tietosuojaviraston olisi tällaisissa tapauksissa ilmoitettava kuukauden kuluessa kuulemispyynnön vastaanottamisesta rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle määräajan jatkamisesta sekä viivästymisen syistä.

4 luku Rekisteröidyn oikeudet

22 §. *Yleisesti saataville asetettava tietosuojaseloste* Pykälässä säädettäisiin yleisesti saataville asetettavasta tietosuojaselosteesta. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 13 artiklan 1 ja 2 kohta. Tietosuojaselosteen tarkoitus on informoida rekisteröityjä ja muita henkilöitä rekisterinpitäjän suorittamasta henkilötietojen käsittelystä ja toteuttaa siten tietojenkäsittelyn avoimuutta. Pykälä vastaisi osittain henkilötietolain rekisteriselostetta koskevaa 10 §:ää. Ehdotettuun tietosuojaselosteeseen kuitenkin sisältyisi sellaisia tietoja, joita ei nykyään tarvitse rekisteriselosteeseen sisällyttää.

Pykälän *1 momentin* mukaan rekisterinpitäjän olisi ylläpidettävä sen vastuulle kuuluvasta henkilötietojen käsittelystä yleisesti saatavilla olevaa kirjallista selostetta, josta käy ilmi vähintään momentissa luetellut tiedot. Kirjallisella selosteella tarkoitetaan myös sähköisessä muodossa olevaa selostetta.

Selosteessa tulisi momentin *1 kohdan* mukaan ilmoittaa ensinnäkin rekisterinpitäjän ja mahdollisen tietosuojavastaavan yhteystiedot ja rekisterinpitäjän harkinnan mukaan tietosuojavastaavan nimi.

Momentin *2 kohdan* mukaan niin sanotuissa yhteisrekisterinpidon tilanteissa tulisi tietosuojaselosteessa ilmoittaa myös yhteisten rekisterinpitäjien yhteyspisteenä toimivan rekisterinpitäjän nimi ja yhteystiedot. Lisäksi tulisi antaa tieto siitä, että rekisteröity voi käyttää ehdotetun lain mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään. Ehdotettu säännös ei perustu direktiivin lainsäädäntötoimeksiantoon, vaan olisi kansallista sääntelyä.

Momentin *3 kohdan* mukaan tietosuojaselosteessa tulisi ilmoittaa henkilötietojen käsittelyn tarkoitukset ja oikeusperuste, kuten esimerkiksi lain säännös, johon henkilötietojen käsittely perustuu.

Momentin *4 kohdan* mukaan selosteesta tulisi käydä ilmi henkilötietojen säilytysaika. Mikäli säilytysajan ilmoittaminen ei ole mahdollista esimerkiksi siksi, että säilytysaika

ei ole numeerisesti määritelty, tulisi selosteessa ilmoittaa sen sijaan säilytysajan määrittämiskriteerit.

Momentin *5 kohdan* mukaan tietosuojaselosteeseen tulee sisällyttää tieto mahdollisista säännönmukaisista henkilötietojen vastaanottajista tai vastaanottajaryhmistä, mukaan lukien kolmansiin maihin sijoittautuneet vastaanottajat sekä kansainväliset järjestöt. Selosteessa ei siten tarvitsisi välttämättä nimetä kaikkia vastaanottajia, joille henkilötietoja mahdollisesti siirretään tai luovutetaan. Riittävää olisi, että selosteesta kävisi ilmi joko yksilöidysti tai asianmukaisesti ryhmiteltynä ne vastaanottajat, joille henkilötietoja kohtalaisen säännönmukaisesti siirretään tai luovutetaan.

Selosteessa tulisi momentin *6 kohdan* mukaan antaa myös tieto siitä, että rekisteröidyllä on oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten henkilötietojen oikaisemista, poistamista tai niiden käsittelyn rajoittamista siten kuin 25 §:ssä säädetäisiin. Momentin *7 kohdan* mukaan selosteessa niin ikään tulisi olla tieto siitä, että rekisteröidyllä on oikeus tehdä 55 §:ssä tarkoitettu kantelu Tietosuojavirastolle, ja viraston yhteystiedot. Selosteeseen tulisi momentin *8 kohdan* mukaan sisällyttää myös mahdolliset muut rekisteröidyn oikeuksien käyttämiseksi tarpeelliset tiedot.

Pykälän *2 momentin* mukaan 1 momentin 4, 5 ja 8 kohdassa tarkoitettujen tietojen antamista voitaisiin viivyttää tai rajoittaa tai ne voidaan jättää antamatta, jos 28 §:ssä säädetty edellytykset täyttyvät. Säännös perustuisi rikosasioiden tietosuojadirektiivin 13 artiklan 3 kohtaan. Pykälän 1 momentissa tarkoitettuja oikeuksia voitaisiin lisäksi rajoittaa erityislainsäädännöllä direktiivin 13 artiklan 3 kohdan mukaisesti. Tiedonsaantioikeuden rajoittaminen voi olla tarpeen etenkin kansallisen turvallisuuden alalla.

23 §. Rekisteröidyn tarkastusoikeus. Pykälässä säädetäisiin rekisteröidyn oikeudesta saada pääsy henkilötietoihin rikosasioiden tietosuojadirektiivin 14 artiklan mukaisesti. Henkilötietolain 26 §:ää vastaten tästä oikeudesta käytettäisiin nimeä tarkastusoikeus.

Pykälässä säädetäisiin, että rekisteröidyllä on oikeus saada rekisterinpitäjältä tieto siitä, käsitelläänkö häntä koskevia henkilötietoja. Tiedon saamiseksi tulisi rekisteröidyn esittää tiedon etsimiseksi tarpeelliset seikat. Tarkastusoikeuden rajoituksista säädetäisiin ehdotetun lain 24 §:ssä.

Lisäksi mikäli rekisteröityä koskevia henkilötietoja käsitellään, olisi rekisteröidyllä oikeus saada rekisterinpitäjältä momentissa luetellut tiedot. Tieto olisi momentin *1 kohdan* mukaan annettava käsiteltävistä henkilötiedoista ja kaikista tietojen alkuperästä käytettävissä olevista tiedoista, kuten siitä, onko tieto peräisin esimerkiksi rekisteröidyltä itseltään vai toiselta viranomaiselta.

Momentin 2 kohdan mukaan rekisteröidylle tulisi ilmoittaa henkilötietojen käsittelyn tarkoitukset ja oikeusperuste, kuten esimerkiksi lain säännös, johon henkilötietojen käsittely perustuu. Pykälän 3 kohdan mukaan rekisteröidylle tulisi antaa myös tieto käsittelyn kohteena olevista henkilötietoryhmistä.

Momentin 4 kohdan mukaan rekisteröidylle annettaviin tietoihin tulisi sisällyttää tieto mahdollisista henkilötietojen vastaanottajista tai vastaanottajaryhmistä, mukaan lukien kolmansiin maihin sijoittautuneet vastaanottajat sekä kansainväliset järjestöt.

Momentin 5 kohdan mukaan rekisteröidylle tulisi ilmoittaa myös henkilötietojen säilytysaika. Mikäli säilytysajan ilmoittaminen ei olisi mahdollista esimerkiksi siksi, että säilytysaikaa ei ole numeerisesti määriteltä, tulisi selosteessa ilmoittaa sen sijaan säilytysajan määrittämiskriteerit.

Rekisterinpitäjän tulisi antaa myös tiedot rekisteröidyn oikeuksien käyttämisestä. Momentin 6 ja 7 kohdan mukaisesti tieto tulisi antaa rekisteröidyn oikeudesta pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista, poistamista tai niiden käsittelyn rajoittamista sekä oikeudesta tehdä 55 §:ssä tarkoitettu kantelu Tietosuojavirastolle ja viraston yhteystiedot.

Pykälän 2 momentissa säädettäisiin 1 momenttiin liittyvästä menettelytavasta. Säännöksen mukaisesti sen, joka haluaa tarkastaa itseään koskevat tiedot 1 momentissa tarkoitettulla tavalla, olisi esitettävä tätä tarkoittava pyyntö rekisterinpitäjälle omakätisesti allekirjoitetulla asiakirjalla tai sitä vastaavalla varmennetulla tavalla tai henkilökohtaisesti rekisterinpitäjän luona. Tarkastuspyyntö tulisi nykytilaa vastaten esittää aina ensin asianomaiselle rekisterinpitäjälle.

24 §. Tarkastusoikeuden rajoitukset. Pykälässä säädettäisiin 23 §:ssä säädetyn tarkastusoikeuden rajoituksista. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 15 artiklan 1, 3 ja 4 kohtaan. Mainitun artiklan mukaan jäsenvaltiot voivat lailla rajoittaa joko kokonaan tai osittain rekisteröidyn tarkastusoikeuden käyttämistä siltä osin ja niin pitkäksi aikaa kuin osittainen tai täydellinen rajoittaminen on välttämätön ja oikeasuhteinen toimenpide demokraattisessa yhteiskunnassa. Tarkastusoikeuden rajoittaminen on nykyäänkin mahdollista henkilötietolain 27 §:n nojalla. Mainitun pykälän 1 momentin 1 kohdan mukaan tarkastusoikeutta ei ole, jos tiedon antaminen saattaisi vahingoittaa valtion turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta taikka haitata rikosten ehkäisemistä tai selvittämistä. Tältä osin oikeustila ei siten merkittävästi muuttuisi.

Pykälän 1 momentin mukaan rekisteröidyn tarkastusoikeutta voitaisiin lykätä tai rajoittaa tai se voitaisiin evätä 28 §:ssä säädetyillä perusteilla. Tarkastusoikeutta voisi olla

tarpeen lykätä esimerkiksi silloin kun asianosaista on kuultu, mutta esitutkinta ei ole vielä päättynyt. Momentissa säädettäisiin, että jos rekisteröidyn tarkastusoikeutta lykätään, rajoitetaan tai se evätään, rekisterinpitäjän olisi ilman aiheutonta viivytystä ilmoitettava tästä rekisteröidylle. Ilmoitus tulisi tehdä kirjallisesti. Myös lykkäämisen, rajoittamisen tai epäämisen perustelut tulisi tässä yhteydessä momentin mukaan ilmoittaa, jollei niiden ilmoittaminen vaaranna epäämisen tai rajoittamisen tarkoitusta.

Tarkastusoikeuden epäämisen veroisena pidettäisiin momentin sitä, että rekisterinpitäjä ei ole kolmen kuukauden kuluessa pyynnön esittämisestä antanut kirjallista vastausta rekisteröidylle. Rikosasioden tietosuojadirektiiviin ei sisälly vastaavaa säännöstä, eli kyse olisi kansallisesta sääntelystä. Vastaava säännös sisältyy kuitenkin henkilötietolain 28 §:n 2 momenttiin. Mikäli rekisteröity ei saisi tietoja kolmen kuukauden kuluessa, hän voisi kääntyä asiassa Tietosuojaviraston puoleen.

Pykälän 2 *momentin* mukaan rekisterinpitäjän tulisi rajoittaessaan rekisteröidyn tarkastusoikeutta ilmoittaa rekisteröidylle tämän oikeudesta tehdä kantelu Tietosuojavirastolle ja käyttää oikeussuojakeinoja tarkastusoikeuden lykkäämisen, rajoittamisen tai epäämisen johdosta, samoin kuin mahdollisesta oikeudesta käyttää tarkastusoikeutta 29 §:n mukaisesti Tietosuojaviraston välityksellä.

Pykälän 3 *momentissa* säädettäisiin rekisterinpitäjän velvollisuudesta säilyttää tieto niistä perusteista, joihin tarkastusoikeuden epääminen tai rajoittaminen perustuu. Näiden tietojen tulisi olla pyynnöstä valvontaviranomaisen saatavilla. Tietojen dokumentoinnilla voitaisiin tarvittaessa jälkikäteen varmistaa, ovatko perusteet tarkastusoikeuden rajoittamiselle olleet käsillä.

25 §. *Henkilötietojen oikaiseminen, poistaminen tai käsittelyn rajoittaminen.* Pykälässä säädettäisiin henkilötietojen oikaisemisesta ja poistamisesta sekä käsittelyn rajoittamisesta siten kuin rikosasioden tietosuojadirektiivin 16 artiklan 1–3 kohdassa edellytetään.

Pykälän 1 *momentin* mukaan rekisterinpitäjän olisi oma-aloitteisesti tai rekisteröidyn vaatimuksesta ilman aiheutonta viivytystä oikaistava tai täydennettävä rekisteröityä koskeva, käsittelyn kannalta virheellinen tai puutteellinen henkilötieto. Rekisteröity voisi saattaa oikaisu- tai täydentämisvaatimuksen vireille hallintolain yleisiä vireillepanosäännöksiä noudattaen. Rekisteröity voisi toimittaa lisäselvitystä, joiden nojalla puutteellista henkilötietoa voitaisiin täydentää. Jos tieto on käsittelyn tarkoituksen kannalta virheellinen tai puutteellinen, olisi se oikaistava tai täydennettävä.

Pykälän 2 *momentissa* säädettäisiin rekisterinpitäjän velvollisuudesta oma-aloitteisesti tai rekisteröidyn vaatimuksesta ilman aiheutonta viivytystä poistaa rekisteröityä kos-

kevat henkilötiedot, jos niiden käsittely on vastoin 3–7 tai 11 §:ssä säädettyä. Mainintaa siitä, että tiedot tulee poistaa rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi ei olisi tarpeellista tehdä, koska lakisääteinen velvoite pitää sisällään sen, että asiasta on erikseen muualla säädetty.

Poistamisen sijasta rekisterinpitäjän olisi momentin mukaan kuitenkin ainoastaan rajoitettava käsittelyä, jos rekisteröity kiistää tietojen paikkansapitävyyden eikä tietojen paikkansapitävyyttä tai virheellisyyttä voida todentaa (momentin 1 kohta) taikka jos henkilötiedot on säilytettävä todistelua varten (momentin 2 kohta). Virheellisiä ja sittemmin korjattuja henkilötietoja voi olla tarve säilyttää myöhempää todistelua varten tai esimerkiksi virkavirheen mahdollista todentamista varten. Käytännössä usein voi esiintyä tilanteita, joissa joko rekisteröidyn tai viranomaisen perustellut oikeudet edellyttävät, että virheellinen tieto säilytetään korjatun tiedon lisäksi.

Pykälän 3 momentissa säädettäisiin, että tilanteissa, joissa käsittelyä on rajoitettu 2 momentin 1 kohdan nojalla, olisi rekisterinpitäjän ennen rajoituksen poistamista ilmoitettava siitä rekisteröidylle.

26 §. *Rekisteröidyn vaatimuksen epääminen.* Pykälässä säädettäisiin rekisteröidyn 25 §:ssä tarkoitetun vaatimuksen epäämisestä ja siihen liittyvistä menettelytavoista siten kuin rikosasioiden tietosuojadirektiivin 16 artiklan 4 kohdassa edellytetään.

Pykälän 1 momentin mukaan tilanteissa, joissa rekisterinpitäjä ei hyväksy rekisteröidyn vaatimusta henkilötietojen oikaisemisesta, täydentämisestä, poistamisesta tai niiden käsittelyn rajoittamisesta, sen tulisi ilmoittaa rekisteröidylle kieltäytymisestä ja sen syistä. Ilmoitus tulisi tehdä kirjallisesti, kuten esimerkiksi kirjeitse tai sähköpostitse. Tiedot kieltäytymisen syistä voitaisiin momentin mukaan kuitenkin kokonaan tai osittain jättää antamatta, mikäli se on välttämätöntä 28 §:ssä säädetyistä syistä.

Pykälän 2 momentissa säädettäisiin rekisterinpitäjän velvollisuudesta ilmoittaa rekisteröidylle tämän käytettävissä olevista oikeussuojakeinoista.

27 §. *Rekisterinpitäjän velvollisuus ilmoittaa oikaisemisesta, poistamisesta tai käsittelyn rajoittamisesta.* Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 16 artiklan 5 ja 6 kohta.

Pykälän 1 momentin mukaan rekisterinpitäjän olisi ilmoitettava virheellisten henkilötietojen oikaisemisesta sille viranomaiselle, jolta virheelliset henkilötiedot ovat peräisin. Näin myös tiedot alun perin luovuttanut viranomainen voi tarvittaessa oma-aloitteisesti oikaista sillä olevat virheelliset henkilötiedot

Pykälän 2 momentissa säädettäisiin, että mikäli henkilötietoja on oikaistu tai poistettu taikka niiden käsittelyä on rajoitettu, tulisi rekisterinpitäjän ilmoittaa tästä niille vastaanottajille, joille rekisterinpitäjä on luovuttanut kyseiset tiedot. Momentissa tarkoitettuihin luovutuksiin sisältyisivät myös mahdolliset henkilötietojen luovutukset kolmansiin maihin. Tiedot saaneen vastaanottajan tulisi omassa toiminnassaan asianmukaisesti huomioida rekisterinpitäjän ilmoittamat henkilötietoihin kohdistuneet toimenpiteet sekä niiden käsittelyyn kohdistuvat rajoitukset, ja esimerkiksi oikaista sillä oleva virheellinen henkilötieto.

28 §. Rekisteröidyn oikeuksien rajoittaminen. Pykälässä säädettäisiin niistä edellytyksistä, joiden täyttyessä eräistä tässä luvussa säädetyistä rekisteröidyn oikeuksista voidaan poiketa. Rekisteröidyn oikeuksia voidaan rajoittaa 24 §:n 1 momentissa, 26 §:n 1 momentissa ja 35 §:ssä tarkoitetulla tavalla, jos se on rekisteröidyn oikeudet huomioon ottaen oikeasuhtaista ja välttämätöntä ja mikäli jokin pykälässä luetelluista tilanteista on käsillä. Oikeuksien rajoittaminen edellyttäisi siten tapauskohtaista punnintaa.

Pykälän 1 kohdan mukaan oikeuksien rajoittaminen olisi sallittua tilanteessa, joissa rajoittamisella vältetään tuottamasta haittaa rikosten ennalta estämiselle, paljastamiselle, tutkimiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle. Kyse voisi olla esimerkiksi tilanteesta, jossa henkilötietojen käsittelyn rajoittaminen vaarantaisi rikostutkinnan toteutumisen.

Pykälän 2 kohdan mukaan rajoittaminen olisi sallittua, jos se on tarpeen viranomaisen muun tutkinnan, selvityksen tai vastaavan menettelyn turvaamiseksi. Kyse voi tällöin olla myös esimerkiksi toisen EU-maan toimivaltaisen viranomaisen valvontamenettelyn turvaamisesta.

Pykälän 3–5 kohdan mukaan rajoittaminen voisi tulla kyseeseen myös yleisen turvallisuuden, kansallisen turvallisuuden tai muiden henkilöiden oikeuksien suojelemiseksi.

29 §. Oikeuksien käyttäminen Tietosuojaviraston välityksellä. Pykälässä säädettäisiin rekisteröidyn oikeudesta käyttää eräitä oikeuksiaan Tietosuojaviraston välityksellä. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 17 artiklan 1 ja 3 kohta.

Pykälän 1 momentissa säädettäisiin rekisteröidyn välillisestä tarkastusoikeudesta. Säännöksen mukaan rekisteröidyllä olisi oikeus pyytää Tietosuojavirastoa tarkastamaan henkilötietojen ja niiden käsittelyn lainmukaisuus, jos rekisteröidyn tarkastusoikeutta on tämän tai muun lain nojalla lykätty, rajoitettu tai evätty, taikka jos rekisterinpitäjä ei hyväksy rekisteröidyn vaatimusta henkilötietojen oikaisemisesta, täydentämi-

sestä, poistamisesta tai rajoittamisesta. Rekisteröity voisi käyttää näitä oikeuksiaan kuitenkin vasta sen jälkeen, kun rekisteröity on yrittänyt käyttää oikeuksiaan itse suhteessa rekisterinpitäjään, mutta rekisterinpitäjä on rajoittanut rekisteröidyn oikeuksien käyttöä joko kokonaan tai osittain. Kuitenkin tilanteissa, joissa rekisteröidyn tarkastusoikeutta on rajoitettu suoraan laissa, tulisi välillisen tarkastusoikeuden käyttö kyseen suoraan, eli rekisteröity voisi lähestyä rekisterinpitäjän sijaan suoraan Tietosuojavirastoa. Asian vireillepanoon ja muuhun käsittelyyn Tietosuojavirastossa sovellettaisiin yleislakina hallintolakia, jollei muualla laissa toisin säädettäisi.

Pykälän 2 *momentin* mukaan tilanteissa, joissa Tietosuojavirasto toimii rekisteröidyn puolesta 1 momentissa tarkoitetuissa tilanteissa, sen olisi ilmoitettava rekisteröidylle toimenpiteistä, joihin se on ryhtynyt asian johdosta. Tietosuojaviraston olisi myös ilmoitettava rekisteröidylle hänen oikeudestaan käyttää oikeussuojakeinoja, joista säädettäisiin lain 8 luvussa.

30 §. Rekisteröidyn oikeuksien käytön edistäminen ja toimenpiteiden maksuttomuus.

Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 12 artikla. Osittain mainitun artiklan vaatimukset tulisivat täytettyä yleisillä hallinto-oikeudellisilla säännöillä. Esimerkiksi hallintolain 23 §:n mukaan asia on käsiteltävä ilman aiheetonta viivytystä ja viranomaisen on esitettävä asianosaiselle tämän pyynnöstä arvio päätöksen antamisajankohdasta sekä vastattava käsittelyn etenemistä koskeviin tiedusteluihin.

Pykälän 1 *momentissa* säädettäisiin rekisterinpitäjän velvollisuudesta edistää rekisteröityjen mahdollisuuksia käyttää puheena olevassa luvussa tarkoitettuja rekisteröidyn oikeuksia. Kaikki rekisteröidylle annettavat ilmoitukset ja henkilötietojen käsittelyä koskevat tiedot olisi säännöksen mukaan lisäksi annettava tiiviisti esitetyssä, ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tiedot olisi toimitettava millä tahansa asianmukaisella tavalla, kuten sähköisesti. Rekisterinpitäjän olisi pääsääntöisesti toimitettava tiedot samassa muodossa kuin pyyntö. Myös rekisterinpitäjän verkkosivustolla olevien tietojen olisi oltava helposti saatavilla ja ymmärrettävissä, mikä edellyttää selkeän ja yksinkertaisen kielen käyttöä. Tällaiset tiedot olisi mahdollisuuksien mukaan mukautettava heikommassa asemassa olevien henkilöiden tarpeisiin.

Pykälän 2 *momentin* mukaan rekisteröidylle annettavien ilmoitusten ja tietojen sekä rekisteröidyn lain mukaisesti tekemien pyyntöjen käsitteleminen olisivat rekisteröidylle lähtökohtaisesti maksuttomia. Jos rekisteröidyn pyynnot olisivat pyyntöjen toistuvuudesta tai muusta syystä kuitenkin ilmeisen kohtuuttomia tai perusteettomia, rekisterinpitäjä voisi periä toimenpiteistä maksun siten kuin valtion maksuperustelaisissa (150/1992) säädetään. Mainitussa laissa säädetään valtion viranomaisten suoritteiden maksullisuuden ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista.

Henkilötietolain 26 §:n nykyisessä 2 momentissa säädetään, että rekisterinpitäjä saa periä tietojen antamisesta korvauksen, jos siitä, kun asianomainen edellisen kerran sai tarkastettavakseen rekisterin tiedot, on kulunut vähemmän kuin yksi vuosi. Tätä useammin rekisterinpitäjälle osoitetut tarkastusoikeutta koskevat pyynnot eivät kuitenkaan välttämättä aina ole kohtuuttomia. Kuitenkin esimerkiksi samansisältöisten pyyntöjen toimittamista monta kertaa lyhyen ajan sisällä voitaisiin lähtökohtaisesti pitää kohtuuttomana, jolloin toimenpiteistä voitaisiin periä maksu.

Pykälän 3 momentissa säädettäisiin, että jos rekisterinpitäjä 2 momentin mukaisesti perii maksun tai kieltäytyy suorittamasta toimenpidettä, sen on tarvittaessa voitava osoittaa pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. Näin ollen rekisterinpitäjän tulisi käytännössä dokumentoida selvitys siitä, minkä vuoksi toimenpiteestä on peritty maksu.

5 luku Tietoturvallisuus

31 §. Henkilötietojen suojaaminen. Pykälässä säädettäisiin yleisestä henkilötietojen suojaamisveloitteesta. Velvollisuus koskisi niin rekisterinpitäjiä kuin henkilötietojen käsittelijöitäkin. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 4 artiklan 1 kohdan f alakohtaan sekä 29 artiklan 1 kohtaan. Tietojen suojaamista koskeva säännös sisältyy nykyisin henkilötietolain 32 §:ään.

Pykälässä säädettäisiin, että rekisterinpitäjän ja henkilötietojen käsittelijän on teknisin ja organisatorisin toimenpitein suojattava henkilötiedot varmistaakseen rekisteröidyn oikeuksiin kohdistuvaa riskiä vastaava tietoturvallisuuden taso. Henkilötiedot olisi erityisesti suojattava oikeudettomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta. Rekisterinpitäjän olisi nykytilaa vastaavasti esimerkiksi määriteltävä tietojen käyttöoikeudet ja otettava käyttöön salasanajärjestelmät tai vastaavat turvajärjestelyt, jotta varmistetaan, että tietoja pääsevät käsittelemään vain ne henkilöt, joilla on siihen oikeus.

Pykälässä tarkoitettuja toimenpiteitä suunniteltaessa, arvioitaessa ja toteutettaessa tulisi asianmukaisesti ottaa huomioon uusin tekniikka, toimenpiteiden toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisen henkilön oikeuksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Suojauksen vaatimustasoa arvioitaessa voitaisiin siten yhtäältä ottaa huomioon suojaukseen käytettävissä olevat tekniset keinot ja niiden aiheuttamat kustannukset. Toisaalta vaadittavaan tietoturvallisuuden tasoon vaikuttaisi myös se, minkälaisia henkilötietoja käsitellään. Esimerkiksi arkaluonteisten henkilötietojen suojaamiseen ja tieto-

turvalliseen käsittelyyn olisi kiinnitettävä erityisen paljon huomiota ja niiden osalta kattavammat suojatoimet ovat pääsääntöisesti perusteltuja. Vaikka henkilötietoja käsiteltäisiinkin muissa kuin automatisoiduissa käsittelyjärjestelmissä, olisi rekisterinpitäjällä ja mahdollisella henkilötietojen käsittelijällä oltava käytössään tehokkaat menetelmät, kuten lokitiedot tai muunlainen seloste, jolla voidaan osoittaa käsittelyn laillisuus, ja jolla mahdollistetaan omaehtoinen valvonta sekä varmistetaan tietojen eheys ja tietoturva.

32 §. *Henkilötietojen suojaaminen automatisoidussa käsittelyssä.* Pykälässä säädetäisiin erityisistä suojaamisvaatimuksista tilanteissa, joissa henkilötietoja käsitellään automatisoidun tietojen käsittelyn avulla. Säännöksillä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 29 artiklan 2 kohta.

Automatisoidun käsittelyn osalta rekisterinpitäjän tai henkilötietojen käsittelijän tulisi 31 §:ssä edellytettyjen vaatimusten lisäksi toteuttaa riskien arvioinnin pohjalta asianmukaiset toimenpiteet henkilötietojen suojaamiseksi. Automatisoidussa käsittelyssä esimerkiksi henkilötietojen käsittelyn rajoittaminen olisi lähtökohtaisesti varmistettava teknisin keinoin. Henkilötietojen käsittelyn rajoittaminen olisi ilmaistava järjestelmässä siten, siitä käy selvästi ilmi, että henkilötietojen käsittely on rajoitettua.

Pykälässä tarkoitettujen toimenpiteiden tarkoituksena olisi evätä asiattomilta pääsy käsittelyssä käytettäviin laitteisiin, estää tietovälineiden luvaton lukeminen, jäljentäminen, muuttaminen tai poistaminen sekä estää henkilötietojen luvaton syöttäminen järjestelmään sekä järjestelmään tallennettujen henkilötietojen luvaton tarkastelu, muuttaminen tai poistaminen. Lisäksi tällaisilla toimenpiteillä tulisi estää asiattomia käyttämästä automatisoituja käsittelyjärjestelmiä tiedonsiirtolaitteiden avulla ja varmistaa, että automatisoidun käsittelyjärjestelmän käyttöön oikeutetut henkilöt pääsevät ainoastaan käyttöoikeuksiensa piiriin kuuluviin henkilötietoihin. Käyttöoikeudet tulisi määrittää tarpeellisuusharkinnan perusteella. Käyttöoikeuksia tulisi myöntää siten ainoastaan siinä laajuudessa kuin henkilö tarvitsee tiettyjä henkilötietoja tehtäviensä suorittamisessa. Käyttöoikeuksien tulisi olla henkilökohtaisia.

Pykälässä tarkoitetuilla suojatoimenpiteillä olisi lisäksi tarkoitus varmistaa, että jälkikäteisestikin on mahdollista tarkistaa ja todeta, minne henkilötietoja on siirretty tai asetettu saataville. Lisäksi niillä tulisi pyrkiä varmistamaan, että jälkikäteen on mahdollista tarkistaa ja todeta, mitä henkilötietoja on syötetty automatisoituihin käsittelyjärjestelmiin, milloin niitä on syötetty ja kuka niitä on syöttänyt.

Ehdotetun sääntelyn mukaan asianmukaisin toimenpitein tulisi myös pyrkiä estämään henkilötietojen oikeudeton lukeminen, jäljentäminen, muuttaminen tai poistaminen tietoja siirrettäessä tai tietovälineitä kuljettaessa. Rekisterinpitäjän ja henkilötietojen käsittelijän tulisi lisäksi varmistaa, että käytetyt järjestelmät voidaan häiriön tapahtu-

essa palauttaa entiselleen ja että järjestelmän toimintahäiriö ei vahingoita tallennettuja henkilötietoja.

33 §. *Henkilötietojen käsittelijän velvollisuus ilmoittaa tietoturvaloukkauksesta.* Pykälässä säädettäisiin henkilötietojen käsittelijän velvollisuudesta ilmoittaa sen havaitsemasta tai sen tietoon tulleesta tietoturvaloukkauksesta. Pykälän mukaan käsittelijän olisi tällöin ilman aiheutonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle. Ehdotettu säännös perustuisi rikosasioiden tietosuojadirektiivin 30 artiklan 2 kohtaan.

34 §. *Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta Tietosuojavirastolle.* Pykälässä säädettäisiin rekisterinpitäjän velvollisuudesta ilmoittaa henkilötietoihin kohdistuneesta tietoturvaloukkauksesta Tietosuojavirastolle. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 30 artiklan 1, 2 ja 5 kohta.

Pykälän 1 momentissa edellytettäisiin, että rekisterinpitäjä ilmoittaa henkilötietojen tietoturvaloukkauksesta Tietosuojavirastolle, paitsi jos loukkauksesta ei todennäköisesti aiheudu vaaraa rekisteröidyn oikeuksille. Henkilötietojen pseudonymisoinnilla ja muilla tekniikoilla, joita käyttämällä tietoja ei enää voida yhdistää tiettyyn rekisteröityyn, voidaan vähentää mahdollisesta tietoturvaloukkauksesta rekisteröidylle aiheutuvan vaaran todennäköisyyttä.

Rekisterinpitäjän olisi pykälän 2 momentin mukaisesti tehtävä 1 momentissa tarkoitettu ilmoitus ilman aiheutonta viivytystä ja joka tapauksessa 72 tunnin kuluessa saatuaan tietoturvaloukkauksen tietoonsa, jos se on mahdollista. Jos ilmoitus tehtäisiin tätä ajankohtaa myöhemmin, ilmoituksessa olisi kerrottava viivytyksen syyt ja perustelut.

Pykälän 3 momentissa säädettäisiin rekisterinpitäjän velvollisuudesta säilyttää tiedot tietoturvaloukkauksista ja niihin liittyvistä seikoista, kuten niiden vaikutuksista ja toteutetuista korjaavista toimenpiteistä.

35 §. *Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta rekisteröidylle.* Pykälässä säädettäisiin velvollisuudesta informoida rekisteröityä tapahtuneesta tietoturvaloukkauksesta siten kuin rikosasioiden tietosuojadirektiivin 31 artiklan 1, 3 ja 5 kohdassa edellytetään.

Pykälän 1 momentissa säädettäisiin, että rekisterinpitäjän tulisi ilman aiheutonta viivytystä ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidylle, mikäli tietoturvaloukkaus todennäköisesti aiheuttaa merkittävän riskin rekisteröidyn oikeuksille. Riskin todennäköisyyttä arvioitaessa tulisi ottaa huomioon muun muassa tietoturvaloukkauksen kohteena olevien henkilötietojen laji, kohteena olevien rekisteröityjen ryhmä sekä

loukkauksen kohteena olleiden tietojen laajuus. Ilmoittamisvelvollisuutta ei kuitenkaan olisi, jos loukkauksen kohteena oleviin henkilötietoihin on sovellettu asianmukaisia teknisiä ja organisatorisia suojatoimenpiteitä tai jos rekisterinpitäjä on loukkauksen jälkeen ryhtynyt toimenpiteisiin sen varmistamiseksi, ettei rekisteröidyn oikeuksiin kohdistuva riski todennäköisesti toteudu.

Rekisterinpitäjä voisi pykälän 2 *momentin* mukaan rekisteröidylle tehtävän ilmoituksen sijaan tiedottaa tietoturvaloukkauksesta julkisella ilmoituksella, jos ilmoituksen tekeminen rekisteröidylle vaatisi kohtuutonta vaivaa. Julkinen ilmoitus voitaisiin tehdä vapaamuotoisella tavalla, mutta valitun tavan tulisi tehokkaalla tavalla tavoittaa rekisteröidyt. Tapauskohteisesti vaatimuksen julkisesta ilmoituksesta saattaa täyttää esimerkiksi ilmoitus rekisterinpitäjän verkkosivujen etusivulla.

Pykälän 3 *momentin* mukaan rekisteröidylle ilmoittamista voitaisiin kuitenkin lykätä tai rajoittaa tai se voitaisiin poikkeuksellisesti jättää kokonaan tekemättä, jos 28 §:ssä säädetyt edellytykset täyttyvät. Koska kyseessä olisi rajoitus rekisteröidyn oikeuksiin, tulisi poikkeusta tulkita tiukasti.

36 §. *Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta toiselle rekisterinpitäjälle.* Pykälässä säädettäisiin rekisterinpitäjän velvollisuudesta ilmoittaa tietoturvaloukkauksesta toiselle rekisterinpitäjälle. Pykälän mukaan rekisterinpitäjän olisi ilman aiheutonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta sellaiselle Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle, jonka toimittamiin tai jolle toimitettuihin tietoihin loukkaus kohdistuu. Tällaiselle toiselle rekisterinpitäjälle olisi ehdotetun säännöksen mukaan aina ilmoitettava tietoturvaloukkauksesta riippumatta siitä, aiheutuuko loukkauksesta todennäköisesti vaaraa rekisteröidyn oikeuksille vai ei.

Ehdotettu säännös perustuu rikosasioiden tietosuojadirektiivin 30 artiklan 6 kohtaan. Mainittu artikla edellyttää säätämistä ainoastaan siitä, että loukkauksesta ilmoitetaan toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjällä. Ehdotetussa pykälässä kuitenkin ulotettaisiin velvollisuus koskemaan myös ilmoituksia kansallisille rekisterinpitäjille.

37 §. *Tietoturvaloukkauksesta annettavan ilmoituksen sisältö.* Pykälässä säädettäisiin tietoturvaloukkauksen johdosta annettavan ilmoituksen sisällöstä. Ilmoitukselle asetetut vähimmäisedellytykset riippuisivat siitä, kenelle ilmoitus tehdään. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 30 artiklan 3 ja 4 kohtaan sekä 31 artiklan 2 kohtaan. Direktiivin 31 artiklan 2 kohta pantaisiin kuitenkin osittain täytäntöön ehdotetun lain 30 §:n 1 momentilla, jonka mukaan kaikki rekisteröidylle annettavat ilmoitukset ja henkilötietojen käsittelyä koskevat tiedot on annettava tiiviisti esitetyssä, ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.

Pykälän 1 *momentissa* säädettäisiin, että Tietosuojavirastolle ja toiselle rekisterinpitäjälle annettavassa ilmoituksessa on kuvattava henkilötietojen tietoturvaloukkaus. Kuvaukseen olisi mahdollisuuksien mukaan sisällytettävä tiedot asianomaisten rekisteröityjen ryhmistä, rekisteröityjen arvioidusta lukumäärästä, henkilötietotyyppien ryhmistä ja henkilötietojen arvioidusta lukumäärästä.

Rekisteröidylle annettavassa ilmoituksessa olisi pykälän 2 *momentin* mukaan kuvattava tietoturvaloukkauksen luonne.

Lisäksi pykälän 3 *momentissa* säädettäisiin, että 1 ja 2 *momentissa* tarkoitetuista ilmoituksista on käytävä ilmi tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa, sekä tietoturvaloukkauksen todennäköiset seuraukset. Ilmoituksessa tulisi myös kuvata ne toimenpiteet, jotka rekisterinpitäjä on toteuttanut tai joita se on ehdottanut tietoturvaloukkauksen johdosta ja tarvittaessa toimenpiteet loukkauksen haittavaikutusten lieventämiseksi.

Pykälän 4 *momentin* mukaan Tietosuojavirastolle ja toiselle rekisterinpitäjälle annettavat tiedot voitaisiin toimittaa useammassa vaiheessa, mikäli tietoja ei kaikilta osin ole mahdollista toimittaa kerralla.

6 luku Tietosuojavastaava

38 §. *Tietosuojavastaavan nimeäminen.* Pykälässä säädettäisiin rekisterinpitäjän velvollisuudesta nimittää tietosuojavastaava siten kuin rikosasioiden tietosuojadirektiivin 32 artiklassa edellytetään.

Pykälän 1 *momentin* mukaan rekisterinpitäjän tulisi nimetä organisaatiolleen tietosuojavastaava. Tietosuojavastaavalla tulisi olla riittävä asiantuntemus henkilötietojen käsittelyä koskevasta lainsäädännöstä ja alan käytänteistä sekä valmiudet hoitaa 40 §:ssä tarkoitetut tehtävät. Useaa toimivaltaista viranomaista varten voitaisiin nimeätä yksi tietosuojavastaava, jos se on perusteltua kun otetaan huomioon viranomaisten organisaatorakenne ja koko. Yhteisen tietosuojavastaavan nimeämisessä tulisi ottaa huomioon, että tietosuojavastaavalla tulee olla mahdollisuus hoitaa tehtävänsä tehokkaasti kaikkien toimivaltaisten viranomaisten osalta.

Tietosuojavastaava voisi olla sellainen rekisterinpitäjän palveluksessa oleva henkilö, joka on saanut erityisen tietosuojaoikeutta ja alan käytänteitä koskevaa koulutusta asiantuntemuksen saamiseksi. Tarvittavan erityisasiantuntemuksen tason voidaan katsoa määräytyvän etenkin rekisterinpitäjän suorittaman tietojenkäsittelyn ja käsiteltävien tietojen edellyttämän suojan perusteella. Tietosuojavastaava voisi kuitenkin olla myös rekisterinpitäjään nähden ulkopuolinen henkilö, joka hoitaa tietosuojavastaavan

tehtäviä toimeksiantosopimuksen perusteella. Tietosuojavastaava voisi suorittaa tehtäviään osa-aikaisesti tai kokoaikaisesti.

Pykälän 2 *momentissa* edellytettäisiin, että rekisterinpitäjä ilmoittaa tietosuojavastaavan yhteystiedot ja niissä tapahtuvista mahdollisista muutoksista Tietosuojavirastolle.

39 §. *Tietosuojavastaavan asema.* Pykälässä säädettäisiin tietosuojavastaavan asemasta ja se perustuisi rikosasioiden tietosuojadirektiivin 33 artiklaan.

Pykälän 1 *momentissa* säädettäisiin, että rekisterinpitäjän on otettava tietosuojavastaava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. Esimerkiksi suunniteltaessa uusia tietojärjestelmähankintoja tulisi tietosuojavastaavalle varata asianmukaisesti mahdollisuus osallistua hankinnan suunnitteluun.

Pykälän 2 *momentin* mukaan rekisterinpitäjän olisi turvattava tietosuojavastaavan toimintaedellytykset tälle 40 §:ssä säädettyjen tehtävien hoitamiseksi sekä annettava pääsy henkilötietoihin ja käsittelytoimiin. Riittävien resurssien määrittelyssä tulisi ottaa huomioon myös esimerkiksi se, että tietosuojavastaava saa riittävät resurssit asiantuntemuksensa ylläpitämiseksi.

40 §. *Tietosuojavastaavan tehtävät.* Pykälässä säädettäisiin tietosuojavastaavan tehtävistä rikosasioiden tietosuojadirektiivin 34 artiklan mukaisesti.

Tietosuojavastaavan tehtävänä olisi pykälän 1 *momentin* 1 *kohdan* mukaan ensinnäkin neuvoa rekisterinpitäjää ja henkilötietoja sen palveluksessa käsitteleviä henkilötietojen suojaa koskevissa asioissa. *Momentin* 2 *kohdan* mukaan tietosuojavastaava myös valvoisi henkilötietojen käsittelyä koskevan sääntelyn ja rekisterinpitäjän henkilötietojen käsittelyyn liittyvien menettelytapojen noudattamista. Näihin tehtäviin kuulisivat esimerkiksi henkilötietojen käsittelyyn liittyvän vastuunjaon noudattamisen valvonta, tietoisuuden lisääminen tietosuoja-asioista ja henkilötietojen käsittelyyn osallistuvan henkilöstön koulutus sekä käsittelyyn liittyvät tarkastukset.

Tietosuojavastaavan tulisi *momentin* 3 *kohdan* mukaan pyydettäessä antaa neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa, että se toteutetaan 20 §:n mukaisesti. Lisäksi tietosuojavastaavan tehtävänä olisi *momentin* 4 *kohdan* mukaan tehdä yhteistyötä Tietosuojaviraston kanssa ja toimia sen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Näihin kysymyksiin kuuluisivat muun muassa 21 §:ssä tarkoitettu Tietosuojaviraston ennakkuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

Pykälän 2 momentissa kuitenkin säädettäisiin, että tietosuojavastaavan tehtävät eivät koske tuomioistuinten lainkäyttötehtävien yhteydessä suorittamaa henkilötietojen käsittelyä. Momentti perustuisi rikosasioiden tietosuojadirektiivin 32 artiklan 1 kohtaan, jonka mukaan jäsenvaltiot voivat vapauttaa tuomioistuimet ja muut riippumattomat oikeusviranomaiset velvoitteesta nimittää tietosuojavastaava näiden hoitaessa lainkäyttötehtäviään. Sääntelyllä pyritäisiin turvaamaan tuomioistuinten riippumattomuus niiden hoitaessa lainkäyttötehtäviään. Sanamuotonsa mukaisesti poikkeus koskisi ainoastaan tuomioistuinten lainkäyttötehtäviä oikeudenkäynneissä, ja muilta osin tietosuojavastaavan tehtävät ja asema olisivat pääsäännön mukaisia tuomioistuimissa-kin niiden käsitellessä henkilötietoja ehdotetun lain piirissä.

7 luku Henkilötietojen siirrot kolmansiin maihin ja kansainvälisille järjestöille

41 §. *Henkilötietojen siirtoja koskevat yleiset periaatteet.* Pykälässä säädettäisiin henkilötietojen siirtoja kolmansiin maihin ja kansainvälisille järjestöille koskevista yleisistä periaatteista. Säännös perustuisi rikosasioiden tietosuojadirektiivin 35 artiklaan sekä 36 artiklan 1 kohtaan.

Henkilötietojen siirtämiseksi katsottaisiin nykytilaa vastaavasti kaikki tilanteet, joissa rekisterinpitäjä saattaa henkilötietoja kolmannessa maassa sijaitsevalle taholle tai kansainväliselle järjestölle. Siirtämiseksi katsottaisiin siten esimerkiksi henkilötietojen siirtäminen sähköpostitse tai muutoin sähköisesti, kuten katseluoikeuden avaaminen sähköisen yhteyden avulla sekä henkilötietojen tallentaminen pilvipalveluun. Varsinaisena luovuttamisena sen sijaan pidettäisiin puolestaan tilanteita, joissa rekisterinpitäjä luovuttaa henkilötiedot toiselle rekisterinpitäjälle. Myös luovuttamista pidettäisiin henkilötietojen siirtämistä.

Henkilötietojen ulkomaille siirtämistä koskisivat säännökset koskevat kaikkea henkilötietojen tosiasiallista siirtämistä ulkomaille. Säännökset kattaisivat siten sekä henkilötietojen varsinaisen luovuttamisen että niiden siirtämisen kolmansille maille esimerkiksi ulkoistamisen seurauksena. Säännösten sovellettavuuteen ei vaikuttaisi siirrettävien tietojen määrä tai siirron kesto. Ainoastaan rekisterinpitäjänä toimiva toimivaltainen viranomainen voisi siirtää henkilötietoja, vaikkakin se voisi antaa henkilötietojen käsittelijälle tehtäväksi siirtää tiedot rekisterinpitäjien puolesta.

Pykälän 1 momentissa säädettäisiin, että toimivaltainen viranomainen saa siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos ehdotetussa laissa tarkoitettuun henkilötietojen käsittelyyn sovellettavia muita säännöksiä noudatetaan ja jos kaikki momentissa luetellut edellytykset täyttyvät. Säännöksessä tarkoitettuihin siirtoihin luettaisiin mukaan henkilötietojen siirrot edelleen toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle.

Momentin 1 kohdassa edellytettäisiin, että siirto on ensinnäkin tarpeen ehdotetun lain 1 §:n 1 momentissa mainittua tarkoitusta varten. Henkilötietoja tulisi siirtää kolmanteen maahan tai kansainväliselle järjestölle siten ainoastaan, jos se on tarpeen laissa lueteltuja tarkoituksia varten, kuten esimerkiksi rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia varten.

Momentin 2 kohdassa ehdotetaan säädettäväksi, että jotta siirto olisi lainmukainen, tulisi henkilötiedot siirtää kolmannen maan rekisterinpitäjälle tai kansainväliselle järjestölle, joka on toimivaltainen käsittelemään henkilötietoja 1 §:n 1 momentissa mainitussa tarkoituksessa. Momentin 3 kohdassa edellytettäisiin lisäksi, että kolmannen maan, jonne henkilötiedot on tarkoitus siirtää, tietosuojan riittävydestä on rikosasioiden tietosuojadirektiivin 36 artiklassa tarkoitettu Euroopan komission voimassaoleva päätös. Jollei tällaista komission voimassaolevaa päätöstä olisi, tulisi joko olla olemassa asianmukaiset suojatoimet ehdotetun 42 §:n mukaisesti tai 43 §:ssä säädettyjen erityistilanteita koskevien poikkeusten pitää tulla sovellettaviksi.

Ehdotetun pykälän 2 momentin mukaan mikäli henkilötiedot on saatu toisesta EU:n jäsenvaltiosta, siirron edellytyksenä on lisäksi, että kyseinen jäsenvaltio on antanut siirrolle etukäteen luvan. Ilman tällaista lupaa tehtävä siirto olisi kuitenkin sallittu poikkeuksellisesti, jos siirto on välttämätön EU:n jäsenvaltion tai kolmannen maan yleiseen turvallisuuteen tai jäsenvaltion olennaisiin etuihin kohdistuvan välittömän ja vakavan uhan estämiseksi, eikä lupaa voida saada ajoissa. Siirrosta olisi kuitenkin ilmoitettava viipymättä ennakkoluvan antamisesta vastaavalle viranomaiselle.

Pykälän 3 momentissa säädettäisiin, että jos henkilötiedot siirretään edelleen muuhun kolmanteen maahan tai muulle kansainväliselle järjestölle, alkuperäisen siirron toteuttanut toimivaltainen viranomainen voisi antaa luvan edelleen siirtämiselle noudattaen, mitä 1 ja 2 momentissa säädetään ja ottaen asianmukaisesti huomioon kaikki merkittävät seikat, kuten rikoksen vakavuus, henkilötietojen alkuperäisen siirron tarkoitus ja henkilötietojen suojan taso siinä kolmannessa maassa tai kansainvälisessä järjestössä, johon tai jolle tiedot siirretään edelleen.

42 §. *Siirto asianmukaisten suojatoimien perusteella.* Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 37 artikla. Pykälän 1 momentin mukaan mikäli komissio ei ole tehnyt 42 §:n 1 momentin 3 kohdassa tarkoitettua päätöstä, henkilötietoja voisi kuitenkin eräissä tilanteissa siirtää kolmanteen maahan tai kansainväliselle järjestölle, jos 41 §:ssä säädettyt muut edellytykset täyttyvät. Siirron edellytyksenä muiden edellytysten lisäksi olisi, että oikeudellisesti sitovassa asiakirjassa määrätään asianmukaisista henkilötietojen suojatoimista tai vaihtoehtoisesti, että rekisterinpitäjä kaikkia henkilötietojen siirtoon liittyviä seikkoja arvioituaan katsoo, että henkilötietojen suojaamiseksi on toteutettu asianmukaiset suojatoimet.

Ehdotetussa 1 momentissa tarkoitettuja oikeudellisesti sitovia välineitä voisivat olla esimerkiksi oikeudellisesti sitovat kahdenväliset sopimukset, jotka on kansallisen lain mukaan pantu täytäntöön. Tällaisessa välineessä tulisi kuitenkin varmistaa tietosuojaa koskevien vaatimusten noudattaminen ja rekisteröityjen oikeuksien kunnioittaminen, kuten mahdollistaa tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot. Asianmukaisten suojatoimien osalta rekisterinpitäjä voisi ottaa huomioon muun muassa sen, että henkilötietojen siirtoihin sovelletaan salassapitovelvollisuutta ja tietyn käsittelytarkoituksen periaatetta, jolla varmistetaan, ettei tietoja käsitellä muita kuin siirron tarkoituksia varten. Lisäksi rekisterinpitäjän olisi otettava huomioon henkilötietojen käyttötarkoitus ja etenkin se, ettei tietoja käytetä esimerkiksi kuolemanrangaistuksen tai muun epäinhimillisen kohtelun määräämiseen.

Pykälän 2 momentissa säädettäisiin, että rekisterinpitäjän on ilmoitettava Tietosuojavirastolle 1 momentin 2 kohdassa tarkoitettujen siirtojen sarjat. Tiedot kyseisistä siirroista olisi säilytettävä, jolloin ne voitaisiin pyynnöstä asettaa Tietosuojaviraston saataville. Tietoihin olisi sisällytettävä ainakin tiedot siirtojen päivämääristä ja ajankohdista, vastaanottaneesta toimivaltaisesta viranomaisesta, siirtojen perusteista sekä siirretyistä henkilötiedoista.

43 §. Erityistilanteita koskevat poikkeukset. Pykälässä säädettäisiin poikkeusperusteista, joiden nojalla henkilötietoja voitaisiin siirtää kolmanteen maahan tai kansainväliselle järjestölle silloin, kun komissio ei ole tehnyt 41 §:n 1 momentin 3 kohdassa tarkoitettua päätöstä eikä 42 §:ssä edellytetyjä asianmukaisia suojatoimia tiedonsiirrolle ole. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 38 artiklaan.

Pykälän 1 momentissa säädettäisiin, että tällöin siirto olisi mahdollinen vain, jos siirto on tarpeen rekisteröidyn tai toisen henkilön elintärkeiden etujen suojaamiseksi, rekisteröidyn oikeutettujen etujen turvaamiseksi taikka EU:n jäsenvaltion tai kolmannen maan yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhkan estämiseksi. Lisäksi momentin 4 kohdan mukaan siirto olisi mahdollinen myös yksittäistapauksissa 1 §:n 1 momentissa mainittuja tarkoituksia varten tai niihin liittyvien oikeusvaateiden laatimiseksi, esittämiseksi tai puolustamiseksi. Sanamuotonsa mukaisesti 4 kohdassa tarkoitettu siirto peruste voisi tulla kyseeseen vain yksittäistapauksessa, eikä säännöstä voitaisi käyttää oikeusperusteena silloin, kun kyse on esimerkiksi säännönmukaisesta tietojensiirrosta.

Pykälän 2 momentissa asetettaisiin kuitenkin velvollisuus suorittaa intressipunnintaa eri oikeuksien välillä ennen kuin henkilötietoja siirretään 1 momentin 4 kohdan mukaisesti. Henkilötietoja ei saa siirtää ehdotetun kohdan nojalla, jos asianomaisen rekisteröidyn oikeuksia on pidettävä siirtoa puoltavaa yleistä etua painavampana.

Tiedot siirroista, jotka perustuvat ehdotettuun 1 momenttiin, olisi pykälän 3 *momentin* mukaan säilytettävä ja asetettava pyynnöstä Tietosuojaviraston saataville. Tällaisiin tietoihin tulisi sisältyä ainakin tiedot siirron päivämäärästä ja ajankohdasta sekä tiedot vastaanottaneesta toimivaltaisesta viranomaisesta, siirron perusteista ja siirretyistä henkilötiedoista.

44 §. *Henkilötietojen siirto kolmansiin maihin yksityisille ja muille vastaanottajille.* Pykälässä säädettäisiin henkilötietojen siirrosta kolmansiin maihin yksityisille ja muille vastaanottajille. Tällaiset vastaanottajat määritelmänsä mukaisesti ovat pääsääntöisesti muita kuin toimivaltaisiin viranomaisiin rinnastettavissa olevia viranomaisia. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 39 artiklaan.

Pykälän 1 *momentissa* säädettäisiin niistä edellytyksistä, joiden täytyessä ehdotetun lain 2 §:n 7 kohdan a alakohdassa tarkoitettu toimivaltainen viranomainen voi yksittäisessä tapauksessa 42 §:n 1 momentin 2 kohdassa säädetyn estämättä siirtää henkilötietoja suoraan kolmansiin maihin sijoittautuneille yksityisille ja muille vastaanottajille. Kaikkien momentissa lueteltujen edellytysten tulisi täytyä samanaikaisesti. Pykälässä tarkoitetut siirrot tulisivat kyseeseen varsin poikkeuksellisesti.

Siirto olisi sallittu ensinnäkin vain silloin, kun se on 1 *kohdan* mukaisesti välttämätön, jotta siirron toteuttava toimivaltainen viranomainen voi suorittaa sille säädetyn 1 §:n 1 momentissa tarkoitettujen tehtävien. Momentin 2 *kohdan* mukaan tietoja siirtävän toimivaltaisen viranomaisen tulisi lisäksi katsoa, että asianomaisen rekisteröidyn oikeudet eivät syrjäytä yleistä etua, jonka perusteella siirto käsiteltävänä olevassa tapauksessa on tarpeen. Siirtävän viranomaisen olisi siis suoritettava asianmukainen intressipunninta tältä osin.

Edellytyksenä siirrolle momentin 3 *kohdan* mukaan olisi, että tietoja siirtävä toimivaltainen viranomainen lisäksi katsoo, että siirto kolmannen maan toimivaltaiselle viranomaiselle olisi asian kiireellisyydestä tai muusta syystä tehoton tai epätarkoituksenmukainen. Momentin 4 *kohdassa* kuitenkin edellytettäisiin, että tällaisen kolmannen maan toimivaltaiselle viranomaiselle ilmoitetaan tapahtuneesta siirrosta ilman aiheutonta viivästystä, jollei tämä ole tehontonta tai epätarkoituksenmukaista.

Momentin 5 *kohdan* mukaan tietoja siirtävän toimivaltaisen viranomaisen olisi ilmoitettava vastaanottajalle, mitä tiettyä tarkoitusta tai tiettyjä tarkoituksia varten tämä saa käsitellä henkilötietoja ja että tietoja saa käsitellä vain sillä edellytyksellä, että tällainen käsittely on tarpeellista. Vastaanottajalle on ilmoitettava myös siitä, ettei tietoja saa käsitellä muita tarkoituksia varten.

Momentin 6 kohdassa edellytettäisiin, että siirto ei saa olla vastoin Suomen kansainvälisiä sopimusvelvoitteita. Lisäksi siirrossa tulisi noudattaa muutoinkin ehdotetun lain muita säännöksiä.

Pykälän 2 momentissa asetettaisiin toimivaltaiselle viranomaiselle velvollisuus säilyttää tiedot 1 momentin nojalla tehdyistä siirrosta sekä ilmoittaa niistä Tietosuojavirastolle. Säännöksessä tarkoitettu ilmoitus olisi tehtävä ilman aiheetonta viivytystä.

8 luku Valvontaviranomainen

45 §. Tietosuojavirasto. Pykälässä säädettäisiin kansallisesta valvontaviranomaisesta lain soveltamisalalla. Kansallinen valvontaviranomainen olisi Suomessa sama elin kuin yleisen tietosuoja-asetuksen ja ehdotetun tietosuojalain alalla, eli Tietosuojavirasto.

Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 41, 42 ja 45 artikla tarpeellisin osin. Suurin osa Tietosuojaviraston organisaatiota koskevista säännöksistä tulisivat säädetyksi ehdotetussa tietosuojalaissa. Esimerkiksi 42 artiklan 5 kohtaa ei ehdoteta tässä laissa täytäntöön pantavaksi, sillä ehdotetussa tietosuojalaissa säädettäisiin Tietosuojaviraston henkilöstöstä ja siitä, että tietosuojavaltuutettu valitsee viraston henkilöstön.

Ehdotetun lain noudattamista valvoisi pykälän 1 momentin mukaan ehdotetun tietosuojalain 7 §:ssä tarkoitettu Tietosuojavirasto.

Pykälän 2 momentissa säädettäisiin, että 8 luvun säännöksiä valvonnasta ei kuitenkaan sovelleta tuomioistuinten lainkäyttötoimintaan. Sääntely perustuu rikosasioiden tietosuojadirektiivin 45 artiklan 2 kohtaan. Sääntelyllä pyritäisiin ennen kaikkea turvaamaan tuomioistuinten riippumattomuus niiden lainkäyttötoiminnassa. Lain 8 luvun säännöksiä sovellettaisiin kuitenkin lain soveltamisalaan kuuluvaan tuomioistuinten suorittamaan henkilötietojen käsittelyyn siltä osin, kun kyse ei ole säännöksessä tarkoitettusta lainkäyttötoiminnasta.

Tuomioistuinten lainkäyttötoiminnan yhteydessä tapahtuvaa henkilötietojen käsittelyä valvottaisiin kuitenkin ylimmän laillisuusvalvonnan kautta. EU:n perusoikeuskirja edellyttää, että riippumaton viranomainen valvoo henkilötietojen suojaa koskevien sääntöjen noudattamista.

Pykälän 3 momentin mukaan Tietosuojavirasto toimisi riippumattomasti hoitaessaan ehdotetussa laissa sille säädettyjä tehtäviä. Tämä tarkoittaisi, että valvontaviranomaisen palveluksessa oleviin ei tulisi voida vaikuttaa ulkopuolelta suoraan eikä välillisesti

näiden hoitaessa tehtäviään ja käyttäessä valtuuksiaan. Näiden ei myöskään tulisi ottaa tältä osin vastaan ohjeita miltään ulkopuoliselta taholta. Riippumattomuuden turvaamiseksi Tietosuojavirastolle olisi myös osoitettava riittävät resurssit, jotta se voi suorittaa tehtävänsä ja käyttää valtuuksiaan tehokkaasti.

46 §. Tehtävät. Pykälässä säädettäisiin Tietosuojaviraston tehtävistä ehdotetun lain soveltamisalalla. Pykälä perustuisi rikosasioiden tietosuojadirektiivin 46 artiklaan. Tietosuojaviraston ehdotetun lain mukaiset tehtävät poikkeaisivat joiltain osin niistä tehtävistä, joita sille on yleisen tietosuoja-asetuksen 59 artiklassa säädetty.

Pykälän *1 momentissa* lueteltaisiin Tietosuojaviraston tehtävät. Niihin kuuluisi ehdotetun lain noudattamisen yleisen valvonnan lisäksi momentin *1 kohdan* mukaan yleisen tietoisuuden lisääminen henkilötietojen käsittelyyn liittyvistä riskeistä, lainsäädännöstä, suojatoimista ja oikeuksista. Momentin *2 kohdan* mukaan Tietosuojaviraston tulisi niin ikään edistää rekisterinpitäjien ja henkilötietojen käsittelijöiden tietoisuutta niille ehdotetun lain mukaan kuuluvista velvollisuuksista. Näitä tehtäviä voitaisiin täyttää esimerkiksi julkaisemalla ohjeistuksia ja kouluttamalla rekisterinpitäjiä.

Tietosuojaviraston tehtäviin kuuluisi momentin *3 ja 4 kohdan* mukaan tietojen antaminen pyynnöstä rekisteröidylle hänelle ehdotetun lain nojalla kuuluvien oikeuksien käyttämiseen liittyen sekä neuvonnan antaminen 21 §:ssä tarkoitetun ennakkokuulemismenettelyn yhteydessä. Tietosuojaviraston tulisi momentin *5 kohdan* mukaan tehdä selvityksiä ehdotetun lain noudattamisesta. Tietosuojavirasto tarkistaisi momentin *6 kohdan* mukaan käsittelyn lainmukaisuuden siten kuin 29 §:ssä säädetään ja ilmoittaisi rekisteröidylle kohtuullisen ajan kuluessa tarkistuksen tuloksesta tai siitä, miksi tarkistusta ei ole tehty.

Momentin *7 kohdan* mukaan Tietosuojavirasto käsittelee rekisteröidyn tai 55 §:n 2 momentissa tarkoitetun yhteisön tekemät kantelut ja tutkisi ne tarpeellisin osin. Viraston tulisi ilmoittaa kantelun tekijälle tutkinnan etenemisestä ja tutkinnan tuloksista kohtuullisen ajan kuluessa. Tietosuojaviraston olisi rikosasioiden tietosuojadirektiivin 46 artiklan 2 kohdan mukaisesti helpotettava tässä kohdassa tarkoitettujen kanteluiden jättämistä toimenpitein, kuten tarjoamalla yleisesti saatavilla oleva kantelulomake esimerkiksi verkkosivuillaan.

Momentin *8 kohdan* mukaan viraston tulisi seurata henkilötietojen suojaan vaikuttavaa teknologista ja muuta kehitystä. Momentin *9 kohdan* nojalla Tietosuojavirasto osallistuisi lisäksi yleisellä tietosuoja-asetuksella perustetun tietosuojaneuvoston toimintaan.

Pykälän *2 momentissa* säädettäisiin, että Tietosuojaviraston toimenpiteet ovat rekisteröidylle ja tietosuojavastaavalle maksuttomia. Jos rekisteröidyn tai tietosuojavastaa-

van pyynnöt kuitenkin olisivat pyyntöjen toistuvuudesta tai muusta syystä ilmeisen kohtuuttomia tai perusteettomia, virasto voisi periä toimenpiteistä maksun siten kuin valtion maksuperustelaissa säädetään tai jättää pyynnön kohteena olevan asian tutkimatta. Asian tutkimatta jättäminen voisi tulla kyseeseen varsin poikkeuksellisesti. Tällainen tilanne voisi olla käsillä esimerkiksi tilanteessa, jossa asia on jo vireillä Tietosuojavirastossa.

Pykälän 3 *momentin* mukaan Tietosuojaviraston olisi tarvittaessa osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus, jos se 2 momentissa tarkoitetulla tavalla perii toimenpiteestä maksun tai jättää asian tutkimatta.

47 §. Tietojensaantioikeus. Pykälässä säädettäisiin Tietosuojaviraston tietojensaantioikeudesta. Pykälällä pantaisiin täytäntöön sekä rikosasioiden tietosuojadirektiivin 26 artikla että 47 artiklan 1 kohta. Rikosasioiden tietosuojadirektiivissä edellytetään, että valvontaviranomaisella on tehokkaat tutkintavaltuudet. Näihin valtuuksiin on sisällyttävä ainakin valtuudet saada rekisterinpitäjältä ja henkilötietojen käsittelijältä pääsy kaikkiin käsiteltävänä oleviin henkilötietoihin ja kaikkiin tietoihin, jotka ovat tarpeen valvontaviranomaisen tehtävien suorittamisessa.

Pykälän 1 *momentissa* säädettäisiin, että Tietosuojavirastolla on oikeus salassapitosäännösten estämättä saada rekisterinpitäjältä ja henkilötietojen käsittelijältä sekä näiden edustajalta maksutta 22 §:ssä tarkoitettu seloste käsittelytoimista, 19 §:ssä tarkoitetut lokitiedot sekä muut tehtäviensä hoitamiseksi välttämättömät tiedot.

Pääpiirteissään vastaavanlainen säännös sisältyy henkilötietolain 39 §:n 1 momenttiin, jonka mukaan tietosuojavaltuutetulla on oikeus salassapitosäännösten estämättä saada tiedot käsiteltävistä henkilötiedoista sekä kaikki tiedot, jotka ovat tarpeen henkilötietojen käsittelyn lainmukaisuuden valvonnassa. Tietosuojalautakunnalla on mainitun lainkohdan mukaan niin ikään vastaava oikeus sen käsiteltävinä olevissa asioissa.

Pykälän 2 *momentissa* säädettäisiin Tietosuojaviraston oikeudesta saada rekisterinpitäjältä ja henkilötietojen käsittelijältä selvitys seikoista, jotka ovat tarpeen Tietosuojaviraston tehtävien hoitamiseksi. Rekisterinpitäjä ja henkilötietojen käsittelijä olisivat lisäksi muutoinkin pyynnöstä velvollisia tekemään yhteistyötä Tietosuojaviraston kanssa sen tehtävien suorittamiseksi.

48 §. Oikeus tehdä tarkastuksia. Pykälässä säädettäisiin Tietosuojaviraston oikeudesta tehdä tarkastuksia siten kuin rikosasioiden tietosuojadirektiivin 47 artiklan 1 ja 4 kohdassa edellytetään. Säännöksellä pyritään turvaamaan Tietosuojaviraston tehokkaat tutkintavaltuudet sekä näihin liittyvien oikeussuojatakeiden toteutuminen.

Pykälän 1 momentin mukaan Tietosuojavirasto voisi tehdä tarkastuksen rekisterinpitäjän ja henkilötietojen käsittelijän toimitiloissa, jos tarkastus on tarpeen ehdotetun lain noudattamisen valvomiseksi. Tarkastuksessa noudatettaisiin, mitä hallintolain (434/2003) 39 §:ssä säädetään.

Tarkastusta ei kuitenkaan saisi tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa. Tältä osin nykytila muuttuisi, sillä henkilötietolain 39 §:n 2 momentin mukaisesti tietosuojavaltuutettu on saanut toimittaa kotirauhan piiriin kuuluvassa tilassa tarkastuksen vain, jos esillä olevassa tapauksessa on ollut olemassa yksilöity syy epäillä henkilötietojen käsittelyä koskevia säännöksiä rikotun tai rikottavan.

Pykälän 2 momentissa säädettäisiin tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 8 §:ää vastaavalla tavalla, että poliisi on velvollinen tarvittaessa antamaan Tietosuojavirastolle virka-apua sille kuuluvien tehtävien suorittamiseksi. Virka-apu voisi tulla kyseeseen esimerkiksi 1 momentissa tarkoitettujen tarkastusten toteuttamisen yhteydessä, jolloin Tietosuojavirasto voisi tarvita poliisilta virka-apua tarkastuskohteeseen pääsemiseksi.

49 §. Asiantuntijoiden käyttö. Pykälä sisältäisi säännökset Tietosuojaviraston oikeudesta käyttää ulkopuolisia asiantuntijoita. Rikosasioiden tietosuojadirektiivi ei nimenomaisesti edellytä, että jäsenvaltion lainsäädännössä säädetään asiasta, mutta säännös on tarpeen Tietosuojaviraston tehtävien tehokkaan toteuttamisen varmistamiseksi.

Pykälän 1 momentin mukaan Tietosuojavirasto voisi tehtäviään hoitaessaan käyttää apunaan asiantuntijoita. Tietosuojavaltuutettu voisi momentin mukaan nimetä asiantuntijaksi suostumuksensa tehtävään antaneen henkilön, jolla on Tietosuojaviraston tehtävän hoitamisen kannalta merkityksellistä asiantuntemusta.

Myös tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 7 §:ssä säädetään tietosuojavaltuutetun ja tietosuojalautakunnan oikeudesta kuulla asiantuntijoita ja pyytää näiltä lausuntoja. Ehdotettua säännöstä täsmennettäisiin nykytilaan verrattuna säätämällä, että asiantuntijalla olisi oltava tehtävän suorittamisen kannalta merkityksellistä asiantuntemusta ja hänen olisi annettava suostumuksensa tehtävään. Ulkopuolista asiantuntijaa voitaisiin käyttää esimerkiksi tilanteessa, jossa tarvittaisiin erityistä tietoa jonkin asian luonteen tai teknologian erityispiirteistä henkilötietojen käsittelyyn liittyvän riskin arvioimiseksi.

Pykälän 2 momentissa säädettäisiin, että 1 momentissa tarkoitettuun asiantuntijaan sovellettavista virkavastuuta koskevista säännöksistä hänen suorittaessaan pykälässä tarkoitettuja tehtäviä.

50 §. Toimenpiteet. Pykälässä säädettäisiin Tietosuojaviraston toimivaltuuksista. Säännös perustuisi rikosasioiden tietosuojadirektiivin 47 artiklaan. Pykälässä ehdotetaan Tietosuojavirastolle laajempia toimivaltuuksia, kuin mitä rikosasioiden tietosuojadirektiivissä edellytetään. Toimivaltuuksien määrittämisessä on pyritty siihen, että ne olisivat soveltuvien osin mahdollisimman yhdenmukaisia yleisessä tietosuojasetuksessa säädettyjen valtuuksien kanssa.

Tietosuojavirasto voisi pykälän mukaan ehdotetun lain soveltamisalalla antaa rekisterinpitäjälle ohjausta 21 §:ssä tarkoitetussa ennakko kuulemismenettelyssä (1 kohta), ilmoittaa rekisterinpitäjälle tai henkilötietojen käsittelijälle ehdotetun lain väitetyistä rikkomisista (2 kohta) sekä varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää siitä, että aiotut käsittelytoimet voivat olla ehdotetun lain vastaisia (3 kohta). Lisäksi pykälän 4 kohdan mukaan Tietosuojavirasto voisi antaa huomautuksen rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos tämä on käsitellyt henkilötietoja lainvastaisesti.

Pykälän 1–4 kohdassa luetellut toimenpiteet olisivat luonteeltaan kevyempiä kuin kohdassa 5–10 luetellut toimenpiteet. Viimeksi mainittujen säännösten nojalla Tietosuojavirasto voisi muun muassa määrätä rekisterinpitäjän tai henkilötietojen käsittelijän noudattamaan rekisteröidyn pyyntöjä, jotka koskevat ehdotettuun lakiin perustuvien oikeuksien käyttöä taikka asettaa väliaikaisen tai pysyvän kiellon tai muun rajoituksen käsittelylle. Lisäksi Tietosuojavirasto voisi määrätä rekisterinpitäjän tai henkilötietojen käsittelijän saattamaan käsittelytoimet ehdotetun lain säännösten mukaisiksi, tarvittaessa määrättyllä tavalla ja kohtuullisen määräajan kuluessa.

Rikosasioiden tietosuojadirektiivin 47 artiklan 5 kohdassa edellytetään, että jäsenvaltio säätää laissa siitä, että kansallisella valvontaviranomaisella on valtuudet saattaa direktiivin nojalla hyväksytyjen säännösten rikkomiset oikeusviranomaisten tietoon ja tarvittaessa panna vireille tai käynnistää oikeustoimet direktiivin nojalla hyväksytyjen säännösten täytäntöönpanemiseksi. Vaikka ehdotettuun lakiin ei otettaisi asiasta nimenomaista säännöstä, olisi Tietosuojavirastolla oikeus tehdä rikosilmoitus, jos se epäilee, että ehdotetun lain säännöksiä on rikottu rangaistavaksi säädetyllä tavalla.

51 §. Uhkasakko. Pykälässä säädettäisiin, että Tietosuojavirasto voi asettaa ehdotetun 50 §:n 5–10 kohdassa tarkoitetun päätöksen sekä 48 §:ssä tarkoitetun tiedonsaantioikeuden tehosteeksi uhkasakon. Uhkasakon asettamisesta ja tuomitsemisesta maksettavaksi säädetään uhkasakkolaissa (1113/1990).

Rikosasioiden tietosuojadirektiivin 57 artiklassa edellytetään, että jäsenvaltiot vahvistavat direktiivin nojalla annettuihin säännöksiin kohdistuvien rikkomusten johdosta määrättävistä seuraamuksista ja että ne toteuttavat kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten tulisi olla tehokkaita, oikea-

suhtaisia ja varoittavia. Pykälässä säädetyn uhkasakon lisäksi seuraamuksina voisi tulla kyseeseen rikosoikeudellinen vastuu sekä vahingonkorvausvastuu.

52 §. Tietosuojaviraston kuuleminen. Pykälä sisältäisi säännökset siitä, millaisissa tilanteissa muiden viranomaisten on kuultava Tietosuojavirastoa. Ehdotus perustuu ennen kaikkea rikosasioiden tietosuojadirektiivin 28 artiklan 2 kohdan ja 47 artiklan 3 kohdan sisältämiin lainsäädäntötoimeksiantoihin. Mainittujen artiklojen mukaisesti jäsenvaltioiden on säädettävä siitä, että valvontaviranomaista kuullaan valmisteltaessa kansallisen parlamentin hyväksyntää varten ehdotusta lainsäädäntötoimenpiteeksi tai tällaiseen lainsäädäntötoimenpiteeseen perustuvaa sääntelytoimenpidettä, joka liittyy käsittelyyn ja että valvontaviranomainen voi omasta aloitteestaan tai pyynnöstä antaa lausuntoja kaikista henkilötietojen suojaan liittyvistä kysymyksistä.

Pykälän 1 *momentissa* säädettäisiin rikosasioiden tietosuojadirektiivin edellyttämällä tavalla, että Tietosuojavirasto voi omasta aloitteestaan tai pyynnöstä antaa lausuntoja lain 1 §:ssä tarkoitettuun henkilötietojen käsittelyyn liittyvistä kysymyksistä.

Pykälän 2 *momentin* mukaan Tietosuojavirastolle olisi varattava tilaisuus tulla kuulluksi valmisteltaessa lain 1 §:ssä tarkoitettua henkilötietojen käsittelyä koskevia lainsäädännöllisiä tai hallinnollisia uudistuksia. Ehdotetun säännöksen tarkoitus on antaa Tietosuojavirastolle mahdollisuus vaikuttaa henkilötietojen käsittelyyn liittyviin lainsäädännöllisiin ja hallinnollisiin uudistuksiin jo niiden valmisteluvaiheessa. Sisällöllisesti vastaava säännös sisältyy henkilötietolain 41 §:n 1 momenttiin.

Pykälän 3 *momentissa* säädettäisiin tuomioistuimelle velvollisuus sen käsiteltävänä olevassa, ehdotetun lain soveltamista koskevassa asiassa varata Tietosuojavirastolle mahdollisuus tulla kuulluksi. Sisällöllisesti vastaava säännös sisältyy henkilötietolain 41 §:n 2 momenttiin.

Momentin toisessa virkkeessä säädettäisiin, että syyttäjän on varattava Tietosuojavirastolle mahdollisuus tulla kuulluksi tämän lain vastaista menettelyä koskevissa asioissa. Henkilötietolain 41 §:n 2 momentin mukaan syyttäjän on kuultava tietosuojavaltuutettua ainoastaan ennen henkilötietolain vastaista menettelyä koskevan syytteen nostamista. Ehdotetun säännöksen nojalla Tietosuojavirastoa olisi kuultava myös tilanteissa, joissa syyttäjä ei päätyisi nostamaan syytettä. Näin ollen syyttäjä voisi kuulla Tietosuojavirastoa ennen kuin se päättää, nostaako se tämän lain vastaista menettelyä koskevan syytteen.

53 §. Keskinäinen avunanto. Pykälässä säädettäisiin keskinäisestä avunannosta valvontaviranomaisten välillä. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 50 artiklan 1, 2 ja 7 kohta.

Pykälän 1 momentissa säädettäisiin, että Tietosuojaviraston on maksutta annettava toisen EU:n jäsenvaltion vastaavalle valvontaviranomaiselle tämän valvontatehtäväänsään välttämättä tarvitsemat henkilötiedot sekä muut tarpeelliset tiedot, ja tarvittaessa muutoinkin avustettava tätä valvonnan toteuttamisessa. Lisäksi Tietosuojaviraston olisi ryhdyttävä muihinkin tarvittaviin toimenpiteisiin tehokkaan keskinäisen yhteistyön varmistamiseksi. Keskinäisen avunannon lähtökohtaisesta maksuttomuudesta huolimatta valvontaviranomaiset voivat keskenään sopia säännöistä, jotka koskevat keskinäisestä avunannosta poikkeuksellisissa olosuhteissa aiheutuvista erityisistä kustannuksista maksettavia korvauksia.

Keskinäinen avunanto kattaisi erityisesti tietopyynnot ja valvontatoimet, kuten kuulemisten, tarkastusten ja tutkimusten toteuttamista koskevat pyynnot. Avunantopyynnössä on esitettävä kaikki tarvittavat tiedot, kuten pyynnön tarkoitus ja perustelut sen esittämiselle. Vaihdettuja tietoja saisi käyttää ainoastaan siihen tarkoitukseen, jota varten niitä on pyydetty. Tietosuojaviraston olisi toimitettava muiden valvontaviranomaisten pyytämät tiedot lähtökohtaisesti sähköisesti vakiomuodossa siten kuin rikosasioiden tietosuojadirektiivin 50 artiklan 6 kohdassa edellytetään.

Pykälän 2 momentin mukaan Tietosuojaviraston olisi vastattava 1 momentissa tarkoitetun valvontaviranomaisen esittämään pyyntöön ilman aiheetonta viivytystä ja joka tapauksessa viimeistään kuukauden kuluttua pyynnön vastaanottamisesta. Tällaisiin toimenpiteisiin voisi kuulua erityisesti asiaankuuluvien tietojen välittäminen tutkimuksen toteuttamisesta.

9 luku Oikeusturva

54 §. Rikkomisista ilmoittaminen. Pykälässä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 48 artikla, jossa edellytetään jäsenvaltioiden säätävän siitä, että toimivaltaiset viranomaiset ottavat käyttöön tehokkaita mekanismeja, jotka kannustavat ilmoittamaan tämän direktiivin rikkomisista luottamuksellisesti. Vastaavaa säännöstä ei sisälly nykyiseen henkilötietojen suojaa koskevaan kansalliseen lainsäädäntöön. Vastaavan kaltaiset ilmoituskanavat, joiden kautta voidaan raportoida lain rikkomisista (engl. *whistleblowing*) ovat kuitenkin pakollisia esimerkiksi luottolaitoksille luottolaitostoiminnasta annetun lain (610/2014) 7 luvun 6 §:n nojalla sekä vakuutusyhtiöille vakuutusyhtiölain (521/2008) 6 luvun 17 a §:n nojalla.

Pykälän 1 momentissa asetettaisiin toimivaltaiselle viranomaiselle velvollisuus ylläpitää menettelytapoja, joita noudattamalla sille voidaan luottamuksellisesti ilmoittaa ehdotetun lain epäilystä rikkomisesta. Ilmoitusmenettelyn tulisi sisältää asianmukaiset ja riittävät toimenpiteet, joilla järjestetään ilmoitusten asianmukainen käsittely. Ilmoitusmenettelyn tulisi myös sisältää ohjeet, joilla turvataan ilmoituksen tekijän henkilöllisyyden suoja. Järjestelmän toimivuus edellyttää, että menettelytavoista on selkeät ohjeet ja että järjestelmä on helposti käytettävä.

Pykälän 2 momentin mukaan toimivaltaisen viranomaisen olisi säilytettävä 1 momentissa tarkoitettua ilmoitusta koskevat tarpeelliset tiedot. Tiedot olisi poistettava viiden vuoden kuluttua ilmoituksen tekemisestä, jollei tietojen edelleen säilyttäminen ole tarpeen rikostutkinnan, vireillä olevan oikeudenkäynnin, viranomaistutkinnan taikka ilmoituksen tekijän tai ilmoituksen kohteena olevan henkilön oikeuksien turvaamiseksi. Tietojen edelleen säilyttämisen tarpeellisuus olisi joka tapauksessa tutkittava viimeistään kolmen vuoden kuluttua edellisestä tarkistamisesta, josta tulisi tehdä merkintä. Vääriksi tai tarpeettomiksi osoittautuneet tiedot olisi kuitenkin poistettava rekisteristä viivytyksettä.

Pykälän 3 momentissa säädettäisiin rajoituksesta rekisteröidyn tarkastusoikeuteen. Jos luonnollinen henkilö on tehnyt toimivaltaiselle viranomaiselle ilmoituksen ehdotetun lain epäilystä rikkomisesta, ilmoittajan henkilöllisyys olisi pidettävä salassa, jos henkilöllisyyden paljastamisesta voitaisiin olosuhteiden perusteella arvioida aiheutuvan ilmoittajalle haittaa, kuten vastatoimenpiteitä tai syrjintää.

Pykälän 4 momentissa säädettäisiin lisäksi, että 3 momentissa tarkoitettussa tilanteessa ei sovellettaisi viranomaisten toiminnan julkisuudesta annetun lain säännöksiä asianosaisen oikeudesta tiedonsaantiin, jos ilmoittajan henkilöllisyyden ilmaiseminen vaarantaisi hänen turvallisuuttaan, etujaan tai oikeuksiaan. Ehdotetulla 3 ja 4 momentilla on tarkoitus suojata ilmoittajan henkilöllisyyttä ja hänen oikeuksiaan sekä kannustaa ilmoittamaan lain rikkomisista.

55 §. Kantelu Tietosuojavirastolle. Pykälässä säädettäisiin rekisteröidyn oikeudesta tehdä kantelu Tietosuojavirastolle. Pykälällä pantaisiin täytäntöön erityisesti rikosasioiden tietosuojadirektiivin 52 artiklan 1 kohta (ehdotettu 1 momentti) sekä 55 artikla (ehdotettu 2 momentti). Mahdollisuus tehdä kantelu kansalliselle valvontaviranomaiselle on merkittävä oikeussuojakeino, josta on rikosasioiden tietosuojadirektiivin mukaan säädettävä jäsenvaltion lainsäädännössä.

Pykälän 1 momentin mukaan rekisteröidyllä olisi oikeus tehdä kantelu Tietosuojavirastolle, jos rekisteröity katsoo, että häneen liittyvässä henkilötietojen käsittelyssä rikotaan ehdotettua lakia. Rekisteröidyn mahdollisuus valittaa lainvastaisesta henkilötietojen käsittelystä Tietosuojavirastolle ei kuitenkaan rajoita muita mahdollisia hallinnolli-

sia muutoksenhakuineja tai oikeussuojakeinoja, kuten esimerkiksi oikeutta valittaa hallintolainkäyttölain mukaisesti hallintoasiassa tehdystä päätöksestä.

Henkilötietolaissa ei nimenomaisesti säädetä vastaavasta yleisestä kantelu-oikeudesta tietosuojavaltuutetulle. Tietosuojavaltuutetun on henkilötietolain 40 §:n 2 momentin mukaan kuitenkin ratkaistava asia, jonka rekisteröity on saattanut 28 (tarkastusoikeuden toteuttaminen) ja 29 §:n (tiedon korjaaminen) nojalla hänen käsiteltäväkseen. Tietosuojavaltuutettu voi antaa rekisterinpitäjälle määräyksen rekisteröidyn tarkastusoikeuden toteuttamisesta tai tiedon korjaamisesta. Rekisteröity ei voi myöskään henkilötietolain mukaan voi saattaa asiaa vireille tietosuojalautakunnassa.

Ehdotetun säännöksen mukaisesti rekisteröity voi tehdä kantelun missä tahansa tilanteessa, jossa hän katsoo häneen liittyvässä henkilötietojen käsittelyssä rikottavan ehdotettua lakia. Valitus voisi koskea esimerkiksi rekisteröidyn tarkastusoikeuden tai tietojen korjausoikeuden toteuttamista taikka käsittelyperusteen laillisuutta. Valituksen tekemiseen noudatettaisiin hallintolain säännöksiä asian vireillepanosta.

Pykälän 2 momentissa säädettäisiin, että kantelun voi rekisteröidyn suostumuksella saattaa Tietosuojaviraston käsiteltäväksi myös yleishyödyllinen henkilötietojen suoja edistävä yhteisö. Tällainen yleishyödyllinen henkilötietojen suoja edistävä yhteisö voisi edustaa useaakin rekisteröityä Tietosuojavirastolle tehtävässä kanteluasiassa. Lainkohta ei rajoittaisi esimerkiksi rekisteröidyn mahdollisuutta käyttää asiamiestä tehdessään kantelun Tietosuojavirastolle.

Ehdotettu lainkohta perustuu rikosasioiden tietosuojadirektiivin 55 artiklaan, jossa veloitetaan säätämään kansallisen prosessioikeuden mukaisesti siitä, että rekisteröidyllä on oikeus valtuuttaa sellainen voittoja tavoittelematon elin, järjestö tai yhdistys, joka on asianmukaisesti perustettu ja jonka sääntömääräiset tavoitteet ovat yleisen edun mukaisia ja joka toimii rekisteröityjen oikeuksien ja vapauksien suojelemisen alalla heidän henkilötietojensa suojan osalta, tekemään kantelu puolestaan ja käyttämään puolestaan direktiivin 52, 53 ja 54 artiklassa tarkoitettuja oikeuksia.

56 §. Kantelun käsitteleminen. Pykälässä säädettäisiin 55 §:ssä tarkoitetun kantelun käsittelemisestä.

Pykälän 1 momentilla pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 46 artiklan 1 kohdan f alakohta sekä 52 artiklan 4 kohta. Tietosuojaviraston tulisi tutkia kantelu sekä ilmoittaa kantelun tekijälle tutkinnan etenemisestä ja tutkinnan tuloksista kohtuullisen ajan kuluessa. Kohtuullista aikaa arvioitaessa merkityksellisiä seikkoja voivat olla esimerkiksi asian laatu ja laajuus.

Tietosuojavirasto ei ehdotetun momentin toisen virkkeen mukaan voisi ottaa tutkittavaksi tuomioistuimessa vireillä olevaa asiaa.

Pykälän 2 *momentissa* säädettäisiin tilanteista, joissa Tietosuojavirasto pitää sillä vireillä olevassa asiassa tarpeellisena selvittää, onko Euroopan komission 41 §:n 1 momentin 3 kohdassa tarkoitettu päätös tietosuojan tason riittävydestä tietosuojadirektiivin mukainen. Tällaisissa tilanteissa Tietosuojaviraston olisi saatettava valvontaa koskeva asia hallinto-oikeuden ratkaistavaksi. Tapaukset olisi niiden oletettavasti vähäisen määrän ja asiassa tarvittavan asiantuntemuksen vuoksi syytä keskittää, minkä vuoksi Tietosuojaviraston tulisi lainkohdan mukaan saattaa asia Helsingin hallinto-oikeuden käsiteltäväksi. Pykälä ei perustuisi suoraan rikosasioiden tietosuojadirektiiviin, vaan unionin tuomioistuimen ennakkoratkaisuun asiassa *Schrems* (C-362/14).

57 §. Muutoksenhaku. Pykälässä säädettäisiin muutoksenhausta. Pykälällä pantaisiin täytäntöön rikosasioiden tietosuojadirektiivin 53 artiklan 1 ja 3 kohta, joilla on tarkoitus turvata henkilön oikeus tehokkaihin oikeussuojakeinoihin kansallista valvontaviranomaista eli Tietosuojavirastoa vastaan.

Pykälän 1 *momentissa* säädettäisiin valitusoikeudesta Tietosuojaviraston päätökseen. Lainkohdan mukaan Tietosuojaviraston päätökseen saisi hakea muutosta valittamalla hallinto-oikeuteen siten kuin hallintolainkäyttölaissa säädetään. Momentti vastaisi siten sisällöllisesti henkilötietolain 45 §:n 1 momenttia, jonka mukaisesti tietosuojavalutetun ja tietosuojalautakunnan päätökseen haetaan muutosta valittamalla hallinto-oikeuteen hallintolainkäyttölain mukaisesti.

Pykälän 2 *momentissa* säädettäisiin, että hallinto-oikeuden päätökseen 56 §:n 2 momentissa tarkoitettussa asiassa saisi hakea muutosta valittamalla korkeimpaan hallinto-oikeuteen siten kuin hallintolainkäyttölaissa säädetään.

Pykälän 3 *momentin* mukaan muuhun hallinto-oikeuden päätökseen saisi sen sijaan hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan. Säännös vastaisi henkilötietolain 45 §:n 2 momenttia. Momentin toisessa virkkeessä säädettäisiin siitä, että myös Tietosuojavirastolla on oikeus hakea muutosta hallinto-oikeuden tekemään päätökseen. Näin osaltaan varmistuttaisiin Tietosuojaviraston tehokkaista keinoista valvoa henkilötietojen suojaa koskevien lakien soveltamista siten kuin rikosasioiden tietosuojadirektiivissä edellytetään.

Pykälän 4 *momentin* mukaan Tietosuojaviraston päätöksessä voitaisiin määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei valitusviranomainen toisin määrää. Näin varmistettaisiin se, että Tietosuojavirastolla olisi mahdollisuus

puuttua tehokkaasti lainvastaiseen henkilötietojen käsittelyyn. Nykyisinkin henkilötietolain 45 §:n 3 momentin mukaan tietosuojalautakunnan päätöksessä voidaan määrätä ehdotettua säännöstä vastaavasti velvollisuudesta noudattaa päätöstä muutoksenhausta huolimatta.

10 luku Erinäiset säännökset

58 §. Vahingonkorvaus. Pykälässä säädettäisiin rekisterinpitäjän velvollisuudesta korvata henkilötietojen lainvastaisesta käsittelystä rekisteröidylle tai muulle henkilölle aiheutunut taloudellinen ja muu vahinko. Rikosasioiden tietosuojadirektiivin 56 artikla velvoittaa jäsenvaltiot säätämään siitä, että jos henkilölle aiheutuu aineellista tai aineetonta vahinkoa lainvastaisesta käsittelystä tai muusta direktiivin nojalla annettuja säännöksiä rikkovasta menettelystä, on hänellä oikeus saada korvaus aiheutuneesta vahingosta rekisterinpitäjältä tai muulta jäsenvaltion lainsäädännön mukaisesti toimivaltaiselta viranomaiselta.

Pykälän 1 momentissa säädettäisiin, että rekisterinpitäjä on velvollinen korvaamaan sen taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle tämän lain vastaisesta henkilötietojen käsittelystä. Nykytilaa vastaavasti korvausvastuu koskisi siten myös muulle henkilölle kuin rekisteröidylle aiheutuneen vahingon korvaamista. Korvausvastuu olisi lainkohdan mukaisesti aina rekisterinpitäjällä.

Ehdotetussa säännöksessä on säilytetty nykyiseen henkilötietolain 47 §:ään sisältyvä rekisterinpitäjän tuottamuksesta riippumaton vahingonkorvausvastuu. Pykälän perusteella olisi korvattava nykytilan mukaisesti esimerkiksi sellainen taloudellinen vahinko, joka rekisteröidylle on aiheutunut virheellisen tiedon käytöstä tai lainvastaisesta tietojen luovuttamisesta. Vastuu koskisi myös kaikesta muusta laittomasta henkilötietojen käsittelystä aiheutuvaa taloudellista ja muuta vahinkoa. Näin ollen vastuu kattaisi myös henkilölle laittomasta henkilötietojen käsittelystä aiheutuneen kärsimyksen.

Pykälän 2 momentti olisi informatiivinen ja ilmaisisi sen, että muutoin oikeudesta saada korvaus vahingosta säädetään vahingonkorvauslaissa (412/1974).

59 §. Rikoslain rangaistussäännökset. Pykälä sisältää viittaussäännöksen rikoslain säännöksiin, jotka voivat tulla kyseeseen lain rikkomisten johdosta määrättävinä seuraamuksina, joista säätämistä edellytetään rikosasioiden tietosuojadirektiivin 57 artiklassa.

Pykälä sisältäisi viittaussäännöksen rikoslain 38 luvun 9 §:ään, jossa säädetään tietosuojarikoksesta. Uutta tietosuojarikosta koskevaa rangaistussäännöstä, jolla kumot-

taisiin nykyinen henkilörekisteririkosta koskeva rangaistussäännös, ehdotetaan hallituksen esityksessä tietosuojalaiksi.

Pykälässä viitattaisiin myös henkilötietolain 48 §:ää vastaavalla tavalla rikoslain 38 luvun 3, 4, 8 ja 8 a §:ään, jossa säädetään rangaistus viestintäsalaisuuden loukkauksesta ja törkeästä viestintäsalaisuuden loukkauksesta sekä tietomurrosta ja törkeästä tietomurrosta. Rangaistus 60 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta tuomittaisiin momentin mukaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla laissa säädetä ankarampaa rangaistusta.

60 §. Vaitiolovelvollisuus. Pykälässä säädettäisiin vaitiolovelvollisuudesta henkilölle, joka on osallistunut henkilötietojen käsittelyyn. Henkilötietojen käsittelyyn osallistunut henkilö ei saa oikeudettomasti ilmaista sivulliselle näin tietoonsa saamiaan henkilötietoja. Tällainen henkilötietojen käsittelyyn osallistuva henkilö voisi olla muun muassa rekisterinpitäjän tai toimivaltaisen viranomaisen palveluksessa oleva henkilö, tietosuojavastaava tai henkilötietoja rekisterinpitäjän lukuun käsittelevä henkilö.

Sisällöllisesti vastaavankaltainen vaitiolovelvollisuussäännös sisältyy nykyisen henkilötietolain 33 §:ään, jonka mukaan se, joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, ei saa henkilötietolain vastaisesti sivulliselle ilmaista näin saamiaan tietoja. Vastaava pykälä sisältyy myös ehdotettuun tietosuojalakiin.

11 luku Voimaantulo- ja siirtymäsäännökset

61 §. Voimaantulo. Pykälä sisältää tavanomaisen voimaantulosäännöksen. Pykälällä pannaan täytäntöön rikosasioiden tietosuojadirektiivin 1 kohta, jonka mukaan jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään 6 päivänä toukokuuta 2018. Jäsenvaltioiden on myös sovellettava näitä säännöksiä mainitusta päivästä lukien.

62 §. Siirtymäsäännökset. Pykälän 1 momentissa säädetään siirtymäsäännöksestä, jonka mukaan ennen 6 päivänä toukokuuta 2016 luodut automatisoidut käsittelyjärjestelmät voidaan saattaa ehdotetun 19 §:n mukaisiksi 6 päivään toukokuuta 2023 mennessä.

Siirtymäsäännös perustuu rikosasioiden tietosuojadirektiivin 63 artiklan 2 kohtaan. Siirtymäsäännöksellä ei ole vaikutusta 6 päivänä toukokuuta 2016 jälkeen luotuihin

automatisoituihin käsittelyjärjestelmiin, jotka on kaikilta osin saatettava ehdotetun lain mukaisiksi 6 toukokuuta 2018 mennessä.

Pykälän 2 *momentin* mukaan lain Tietosuojavirastoa koskevia säännöksiä sovellettaisiin vasta ehdotetun tietosuojalain tultua voimaan. Siihen saakka lain noudattamista valvoisi tietosuojavaltuutettu siten kuin henkilötietolaissa säädetään.

Yleistä tietosuoja-asetusta ja sitä täydentävää tietosuojalakia aletaan soveltaa vasta 25.5.2018. Täten siirtymäsäännös on tarpeellinen, jotta tässä ehdotetun lain ja tietosuojalain voimaantulon välisenä aikana henkilötietojen käsittelyn valvonta tulee turvatuksi.

9.2 Rikosrekisterilaki

1 §. *Rikosrekisterin tarkoitus ja tiedot.* Pykälän 1 *momentin* sanamuotoa ehdotetaan täsmennettävän siten, että siinä todettaisiin nimenomaisesti Oikeusrekisterikeskuksen olevan rekisterinpitäjä rikosrekisterin osalta. Oikeusrekisterikeskukseen kohdistuisivat siten rikosrekisterin osalta ehdotetussa yleislaissa rekisterinpitäjälle säädettävät velvollisuudet. Voimassa olevassa rikosrekisterilaissa säädetään Oikeusrekisterikeskuksen pitävän yllä rikosrekisteriä siten kuin siinä laissa säädetään.

6 §. Rikosrekisterilain 6 §:n 8 *momentista* ehdotetaan ensinnäkin poistettavan säännökset rekisteröidyn tarkastusoikeudesta. Asiasta säädettäisiin vastaisuudessa ehdotetussa yleislaissa. Momentissa nykyisin olevaa sääntelyä oikeudesta saada oikeushenkilöä koskeva ote rikosrekisteristä tarkistettaisiin siten, että sen sanamuodosta kävisi selkeämmin ilmi, ettei asiassa ole kyse rekisteröidyn tarkastusoikeudesta. Ehdotettu muutos on luonteeltaan tekninen.

9.3 Laki rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä

4 §. *Suhde muihin lakeihin ja kansainvälisiin velvoitteisiin.* Pykälän 3 *momenttia* ehdotetaan muutettavan siten, että kumottavan henkilötietolain sijasta siinä viitattaisiin ehdotettuun yleislakiin (1. lakiehdotus).

8 §. *Säilytysrekisterin käyttötarkoitus.* Pykälän ensimmäisen virkkeen sanamuotoa tarkistettaisiin niin, että siitä ilmenisi selkeämmin Oikeusrekisterikeskuksen rooli säilytysrekisterin rekisterinpitäjänä. Muutoin pykälä ehdotetaan säilytettävän ennallaan.

13 §. *Tarkastusoikeus.* Pykälän tarkastusoikeutta koskeva sääntely ehdotetaan korvattavaksi informatiivisella säännöksellä, jonka mukaan henkilön oikeudesta tarkastaa häntä koskevat rekisteritiedot säädetään erikseen.

9.4 Laki oikeushallinnon valtakunnallisesta tietojärjestelmästä

2 §. *Suhde muuhun lainsäädäntöön.* Pykälän 1 momenttia ehdotetaan muutettavaksi siten, että kumottavan henkilötietolain sijasta siinä viitattaisiin yleiseen tietosuojasetukseen, tietosuojalakiin sekä ehdotettuun yleislakiin.

10 §. *Tietojärjestelmään talletettavat henkilötiedot.* Pykälän 2 momenttia ehdotetaan muutettavaksi siten, että kumottavan henkilötietolain arkaluonteisten tietojen määritelmään viittaamisen sijasta siinä viitattaisiin yleisen tietosuojasetuksen 9 artiklan arkaluonteisten tietojen määritelmään.

18 §. *Tietojen poistaminen.* Pykälän 2 momentti ehdotetaan kumottavaksi. Momentissa säädetään nykyisin raportointi-, tilasto- ja arkistojärjestelmään talletettujen tietojen poistamisesta sen mukaan kuin henkilötietolaissa säädetään. Henkilötietolaki on tarkoitus kumota, ja koska näistä asioista säädettäisiin vastaisuudessa henkilötietojen käsittelyä koskevissa yleislaeissa, voidaan momentti kokonaisuudessaan kumota.

19 §. *Tarkastusoikeuden toteuttaminen ja tietojen korjaaminen.* Pykälän sääntely tarkastusoikeuden toteuttamisesta ja tietojen korjaamisesta korvattaisiin informatiivisella säännöksellä, jonka mukaan rekisteröidyn tarkastusoikeudesta ja oikeudesta saada itseään koskevat tiedot oikaistua tai täydennettyä säädetään erikseen.

9.5 Laki sakon täytäntöönpanosta

46 §. *Sakkorekisterin käyttötarkoitus ja rekisterin tietojen käsittely.* Pykälän 3 momenttia ehdotetaan tarkistettavaksi siten, että sen nykyinen informatiivinen viittaus kumotavaan henkilötietolakiin korvattaisiin informatiivisella viittauksella yleiseen tietosuojasetukseen, henkilötietolakiin ja ehdotettuun yleislakiin.

49 §. *Vastuu sakkorekisteriin talletetuista tiedoista.* Pykälän sääntely rekisterinpitäjän vahingonkorvaus- ja muusta vastuusta ehdotetaan kumottavaksi, koska vastaisuudessa näistä seikoista säädettäisiin soveltuvassa yleislainsäädännössä.

9.6 Laki henkilötietojen käsittelystä Rikosseuraamuslaitoksessa

1 §. *Lain soveltamisala.* Pykälän viittaussäännös henkilötietolakiin ehdotetaan muutettavaksi viittaukseksi yleiseen tietosuoja-asetukseen, tietosuojalakiin sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettavaan lakiin.

30 §. *Tietojen käsittelystä ilmoittaminen.* Pykälän henkilötietolakiin kohdistuva viittaussäännös ehdotetaan muutettavaksi viittaukseksi yleiseen tietosuoja-asetukseen ja tietosuojalakiin.

31 §. *Tarkastusoikeuden rajoitukset.* Pykälän 1 momentin viittaus henkilötietolakiin ehdotetaan muutettavaksi uuden henkilötietolainsäädännön mukaiseksi.

Pykälän 2 momenttiin tehtäisiin tietosujalain mukainen tietosuojaviranomaisen nimeä ja toimivaltaa koskeva muutos, jonka mukaan Tietosuojavirasto voisi rekisteröidyn pyynnöstä tarkastaa 1 momentissa tarkoitettujen rekisteröityä koskevien tietojen lainmukaisuuden. Voimassa olevassa laissa kyseinen toimivaltuus kuuluu tietosuojavaltuutetulle.

33 §. *Virheelliseksi todetun tiedon säilyttäminen.* Pykälän 1 momenttiin sisältyvä viittaus henkilötietolakiin ehdotetaan muutettavaksi viittaukseksi uuteen henkilötietolainsäädäntöön.

37 §. *Rangaistussäännökset.* Pykälän 2 momentin ensimmäisessä virkkeessä viitataan nykyisin rikoslain henkilörekisteririkosta ja henkilörekisteriin kohdistuvaa tietomurtoa koskeviin säännöksiin. Tietosujalakia koskevassa esityksessä ehdotetaan henkilörekisteririkos korvattavaksi tietosujarikos-nimikkeisellä rangaistussäännöksellä. Tämä käsittemuutos tehtäisiin myös puheena olevaan 2 momenttiin. Mainitun momentin viimeisen virkkeen mukaan rangaistus henkilörekisteririkkomuksesta tuomiin henkilötietolain 48 §:n 2 momentin mukaan. Tietosujalakiin ei ehdoteta otettavaksi säännöksiä tietosujarikkomuksesta, joten kyseinen viittaussäännös poistettaisiin.

9.7 Ulosottokaari

27 §. *Oikeus käsitellä tietoja.* Pykälän 1 momenttiin sisältyvä viittaus henkilötietolakiin ehdotetaan muutettavaksi viittaukseksi uuteen henkilötietolainsäädäntöön.

28 §. *Rekisteröidyn tarkastusoikeuden rajoittaminen.* Pykälän 1 momenttiin ehdotetaan otettavan informatiivinen viittaus siitä, että rekisteröidyn tarkastusoikeudesta säädetään yleisessä tietosuoja-asetuksessa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa. Muutoin momentin sääntely säilyisi ennallaan. Nykyisen 2 momentin sääntelyä ei ehdoteta otettavan pykälään, koska Tietosuojaviraston oikeudesta tarkastaa rekisterissä olevien rekisteröityjen tietojen lainmukaisuus säädettäisiin vastaisuudessa muualla. Pykälän otsikkoa tarkistettaisiin sen ehdotettua pääasiallista sisältöä vastaavaksi.

10 Voimaantulo

Rikosasioiden tietosuojadirektiivin 63 artiklan 1 kohdan mukaan jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään 6 päivänä toukokuuta 2018, mistä lähtien jäsenvaltioiden on myös sovellettava näitä säännöksiä. Tämän johdosta lakien ehdotetaan tulevan voimaan 6 päivänä toukokuuta 2018.

Ennen 6 päivänä toukokuuta 2016 luodut automatisoidut käsittelyjärjestelmät on kuitenkin mahdollista saattaa ehdotetun 19 §:n mukaisiksi 6 päivään toukokuuta 2023 mennessä. Ehdotettu siirtymäsäännös perustuu rikosasioiden tietosuojadirektiivin 63 artiklan 2 kohtaan.

11 Suhde perustuslakiin ja säätämisyjärjestys

Henkilötietojen suoja

Esityksessä ehdotettu sääntely on merkityksellistä perustuslain 10 §:ssä säädetyn yksityiselämän ja henkilötietojen suojan kannalta. Ehdotettu sääntely konkretisoi soveltamisalallaan näitä perustuslain säännöksiä sekä turvaa tältä osin perustuslain 22 §:ssä edellytetyllä tavalla perus- ja ihmisoikeuksien toteutumista.

Ehdotettu sääntely on merkityksellistä myös esimerkiksi EU:n perusoikeuskirjan kannalta. EU:n perusoikeuskirjan 8 artiklassa turvataan jokaisen oikeus henkilötietojensa suojaan. Artiklan mukaan henkilötietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla.

Ehdotuksella toimeenpantaisiin kansallisesti EU:n rikosasioiden tietosuojadirektiivi. Perustuslakivaliokunta katsoi direktiiviehdotuksesta antamassaan lausunnossa, että ehdotuksen aineellinen sisältö noudattelee ja konkretisoi varsin hyvin EU:n perusoikeuskirjan 8 artiklan määräyksiä henkilötietojen suojasta. Edelleen perustuslakivaliokunta katsoi, ettei ehdotus ollut ongelmallinen myöskään perustuslain 10 §:n 1 momentin ja sitä tarkentavan valiokunnan käytännön näkökulmasta (PeVL 12/2012 vp).

Perustuslakivaliokunta on arvioidessaan henkilötietojen suojaa koskevaa sääntelyä katsonut, että tällaista sääntelyä on tarkasteltava perustuslain 10 §:n kannalta. Pykälän 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa (mm. PeVL 31/2017 vp, PeVL 5/2017 vp).

Valiokunta on käytännössään pitänyt henkilötietojen suojan kannalta tärkeinä sääntelykohteina ainakin rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia mukaan luettuna tietojen luovutettavuus sekä tietojen säilytysaikaa henkilörekisterissä ja rekisteröidyn oikeusturvaa. Näiden seikkojen sääntelyn lain tasolla tulee lisäksi olla kattavaa ja yksityiskohtaista (ks. esim. PeVL 31/2017 vp, PeVL 13/2016 vp). Ehdotetun yleislain (1. lakiehdotus) kannalta on olen-

naista, ettei perustuslakivaliokunnan käsityksen mukaan ole estettä sille, että henkilötietojen suojaan liittyvät sääntelyn kattavuuden sekä täsmällisyyden ja tarkkarajaisuuden vaatimukset voidaan joiltain osin täyttää kansalliseen oikeuteen sisältyvällä yleislilla (mm. PeVL 31/2017 vp, PeVL 5/2017 vp).

Ehdotettua yleislakia sovellettaisiin rikosasian yhteydessä tapahtuvaan henkilötietojen käsittelemiseen. Sitä sovellettaisiin myös puolustusvoimien, Rajavartiolaitoksen ja poliisin kansallisen turvallisuuden ylläpitämisen yhteydessä suoritettavaan henkilötietojen käsittelyyn. Ehdotettua yleislakia on tarkoitus täydentää eri hallinnonalojen erityislainsäädännöllä, jossa tarvittavilta osin säädettäisiin tarkemmin esimerkiksi rekisteröivästä henkilötiedoista, niiden käyttötarkoituksista, henkilötietojen luovuttamisesta ja tietojen poistamisesta. Sovellettavaksi tulevaa lainsäädäntöä onkin tarkasteltava kokonaisuutena, mistä johtuen asiaa koskevat esitykset on pyritty valmistelemaan mahdollisimman yhtäaikaaisesti.

Ehdotettuun yleislakiin otettaisiin säännökset henkilötietojen käsittelyn yleisistä edellytyksistä, kuten laillisuusvaatimuksesta, käyttötarkoitussidonnaisuudesta, tarpeellisuusvaatimuksesta, virheettömyysvaatimuksesta, eräiden henkilötietojen toisistaan erottamisesta ja henkilötunnuksen käsittelystä. Henkilötietojen käsittelyn yleisenä edellytyksenä on, että siitä säädetään laissa ja että se on tarpeen toimivaltaisen viranomaisen ehdotetun lain soveltamisalalla tapahtuvan tehtävän suorittamiseksi.

Lakiin ehdotetaan otettavaksi myös säännökset erityisiä henkilötietoja (ns. arkaluonteiset tiedot) koskevan käsittelyn edellytyksistä. Perustuslakivaliokunta on tulkintakäytännössään painottanut tällaisten henkilötietojen käsittelyn aiheuttamia uhkia. Valiokunnan mielestä esimerkiksi arkaluonteisina tietoina pidettävien biometrinen tunnistuksen rekisteröinti merkitsee erityistä tarvetta huolehtia järjestelmään talletettavien henkilötietojen suojaamisesta väärinkäytön vaaroilta ja kaikenlaiselta tietojen laittomalta saannilta ja käytöltä (PeVL 13/2017 vp, s. 5, PeVL 29/2016 vp, s. 5). Valiokunta on kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on syytä rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään (ks. esim. PeVL 13/2017 vp, s. 5 ja PeVL 3/2017 vp, s. 5). Ehdotetussa yleislaissa säädettäisiin, että arkaluonteisia henkilötietoja saa käsitellä vain tietyin laissa säädettävien edellytyksin ja vain, jos niiden käsitteleminen on välttämätöntä. Arkaluonteisten tietojen käsitteleminen edellyttäisi myös, että rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu.

Ehdotettuun yleislakiin otettaisiin myös säännökset rekisterinpitäjän ja henkilötietojen käsittelijän vastuusta, kuten velvollisuudesta säilyttää lokitiedot automaattisessa tietojenkäsittelyjärjestelmässä suoritetusta henkilötietojen keräämisestä, muuttamisesta ja kyselystä. Rekisterinpitäjän olisi ennen henkilötietojen käsittelyn aloittamista arvioita-

va suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojaan sekä eräin edellytyksin kuultava Tietosuojavirastoa aiotusta käsittelystä.

Ehdotettuun yleislakiin otettaisiin säännökset myös rekisteröidyn tarkastusoikeudesta ja oikeudesta saada henkilötiedot oikaistua tai poistettua sekä säännökset rekisteröidyn edellä mainittujen oikeuksien rajoittamisesta. Rekisteröidyllä olisi oikeus kannella ehdotettua yleislakia valvovalle Tietosuojavirastolle, jos rekisteröity katsoo häneen liittyvässä käsittelyssä rikotun ehdotettua lakia. Tietosuojavirastolla olisi mahdollisuus esimerkiksi antaa rekisterinpitäjälle huomautus taikka määrätä henkilötietojen oikaisemisesta tai rajoittamisesta, ja se voisi tarvittaessa tehostaa oikeudellisesti velvoittavaa päätöstään uhkasakolla. Rekisteröidyllä olisi oikeus saada korvausta rekisterinpitäjältä siitä taloudellisesta ja muusta vahingosta, joka on aiheutunut hänelle ehdotetun lain vastaisesta henkilötietojen käsittelystä. Kyse olisi rekisterinpitäjän kannalta tuottamuksesta riippumattomasta ns. ankarasta vahingonkorvausvastuusta.

Lakiin otettaisiin myös yksityiskohtaiset tietoturvallisuutta koskevat säännökset sekä säännökset vaatimuksesta nimetä tietosuojavastaava. Laissa säädettäisiin myös niistä yksityiskohtaisista edellytyksistä, joiden vallitessa henkilötietoja saa siirtää kolmansiin maihin tai kansainvälisille järjestöille.

Kotirauhan suoja

Säädettäväksi ehdotetun yleislain 48 §:ssä on säännös Tietosuojaviraston mahdollisuudesta tehdä tarkastuksia ehdotetun lain noudattamisen valvomiseksi. Tarkastuksia ei kuitenkaan saisi tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa. Ehdotus ei ole ongelmallinen kotirauhan suojaa koskevan perustuslakisääntelyn kannalta (PeVL 43/2010 vp, PeVL 40/2010 vp, PeVL 18/2010 vp, PeVL 6/2010 vp). Tarkastustoiminnassa on noudatettava hallintolain 39 §:n säännöksiä tarkastuksista. Sääntely täyttää tältäkin osin perustuslakivaliokunnan käytännössä asetetut vaatimukset (PeVL 11/2013 vp).

Johtopäätös

Esitykseen sisältyvät lakiehdotukset voidaan hallituksen mielestä käsitellä tavallisen lain säätämisyjärjestyksessä. Esityksessä ehdotettu sääntely on kaiken kaikkiaan valtiosääntöoikeudellisesti merkityksellistä perustuslain 10 §:ssä säädetyn yksityiselämän ja henkilötietojen suojan kannalta, ja sääntelyllä on liittymäkohtia myös muihin perusoikeuksiin. Esitys on näistä syistä aiheellista saattaa eduskunnan perustuslakivaliokunnan käsiteltäväksi.

Edellä esitetyn perusteella annetaan Eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

LAKIEHDOTUKSET

1.

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltaisala

Tätä lakia sovelletaan toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kyse on:

1. rikoksen ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta;
2. syyteharkinnasta ja muusta rikokseen liittyvästä syyttäjän toiminnasta;
3. rikosasian käsittelemisestä tuomioistuimessa;
4. rikosoikeudellisen seuraamuksen täytäntöönpanemisesta; tai
5. yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä kohdassa 1–4 tarkoitetun toiminnan yhteydessä.

Sen lisäksi, mitä 1 momentissa säädetään, tätä lakia sovelletaan:

1. Puolustusvoimien suorittamaan ja Puolustusvoimien lukuun suoritettavaan henkilötietojen käsittelyyn, kun tietoja käsitellään puolustusvoimista annetun lain (551/2007) 2 §:n 1 momentissa säädettyjen tehtävien hoitamiseksi;
2. Poliisin suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään poliisilain (872/2011) 1 §:n 1 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen; ja
3. Rajavartiolaitoksen suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään rajavartiolain (578/2005) 3 §:n 2 ja 3 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen.

Edellä 2 momentissa tarkoitettuun henkilötietojen käsittelyyn ei kuitenkaan sovelleta tämän lain 7 lukua.

Tätä lakia sovelletaan kuitenkin vain sellaiseen 1 ja 2 momentissa tarkoitettuun henkilötietojen käsittelyyn, joka on kokonaan tai osittain automaattista tai jossa käsiteltävät tiedot muodostavat tai niiden on tarkoitus muodostaa rekisteri tai sen osa.

Tällä lailla pannaan täytäntöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta (*tietosuojadirektiivi*).

2 §

Suhde muuhun lainsäädäntöön

Jos muussa laissa on tästä laista poikkeavia säännöksiä, niitä sovelletaan tämän lain asemesta.

Oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999).

3 §

Määritelmät

Tässä laissa tarkoitetaan:

1. *henkilötiedoilla* kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (*rekisteröity*) välittömästi tai välillisesti liittyviä tietoja;
2. *käsittelyllä* tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista sekä muuta toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin;

3. *käsittelyn rajoittamisella* tallennettujen henkilötietojen merkitsemistä tarkoitukseen rajoittaa niiden myöhempää käsittelyä;
4. *rekisterillä* mitä tahansa jäsenneiltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, riippumatta siitä, onko tietojoukko keskitetty, hajautettu taikka toiminnallisin tai maantieteellisin perustein jaettu;
5. *toimivaltaisella viranomaisella* kaikkia viranomaisia, joiden toimivalta kattaa rikosten ennalta estämisen, paljastamisen, selvittämisen tai syyteharkintaan saattamisen, syyteharkinnan ja muun rikoksesta syyttämiseen liittyvän toiminnan, rikosoikeudellisiin seuraamuksiin tuomitsemisen tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy, samoin kuin Puolustusvoimia, poliisia ja Rajavartiolaitosta näiden hoitaessa 1 §:n 2 momentissa tarkoitettuja tehtäviä;
6. *rekisterinpitäjällä* toimivaltaista viranomaista, joka yksin tai yhdessä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot tai jonka tehtäväksi rekisterinpito on lailla säädetty;
7. *henkilötietojen käsittelijällä* luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun;
8. *vastaanottajalla* luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja, lukuun ottamatta sellaista toimivaltaista viranomaista, joka mahdollisesti saa henkilötietoja tämän lain 1 §:n 1 momentin mukaisia tarkoituksia varten tietyn tutkinnan puitteissa;
9. *henkilötietojen tietoturvaloukkauksella* tietoturvallisuutta koskevien säännösten rikkomista, josta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai oikeudeton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin;
10. *asianmukaisilla suojatoimenpiteillä* sellaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan henkilötietojen käsittelyn lainmukaisuus, kun otetaan huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityjen oikeuksiin kohdistuvat riskit;
11. *geneettisillä tiedoilla* henkilötietoja, jotka koskevat sellaisia luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista selviää yksilöllistä tietoa kyseisen luonnollisen henkilön fysiologiasta tai terveydentilasta, ja jotka on saatu kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla tai muutoin;
12. *biometrisillä tiedoilla* luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa;
13. *terveyttä koskevalla tiedoilla* luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, jotka ilmaisevat hänen terveydentilansa;
14. *kolmannella maalla* muuta maata kuin Euroopan unionin (EU) jäsenvaltiota, muuta Euroopan talousalueen maata tai Sveitsiä;

15. *kansainvälisellä järjestöllä* sellaista järjestöä ja sen alaisia elimiä, joihin sovelletaan kansainvälistä julkisoikeutta, sekä muuta elintä, joka on perustettu kahden tai useamman maan välisellä sopimuksella tai tällaisen sopimuksen perusteella.

Mitä tässä laissa säädetään toimivaltaisesta viranomaisesta, sovelletaan myös 1 momentin 5 kohdassa tarkoitettua tehtävää hoitavaan yksityiseen.

Mitä tässä laissa säädetään EU:n jäsenvaltiosta, sovelletaan myös muihin Euroopan talousalueeseen kuuluviin maihin ja Sveitsiin.

2 luku

Henkilötietojen käsittelyn yleiset edellytykset

4 §

Laillisuusvaatimus

Henkilötietoja saa käsitellä vain, jos käsittelystä säädetään laissa ja se on tarpeen toimivaltaisen viranomaisen 1 §:ssä tarkoitetun tehtävän suorittamiseksi.

Henkilötietoja tulee käsitellä asianmukaisesti ja huolellisesti.

5 §

Käyttötarkoitussidonnaisuus

Henkilötietoja saa kerätä vain tiettyjä nimenomaisia tarkoituksia varten, eikä niitä saa käsitellä kyseisten tarkoitusten kanssa yhteensopimattomalla tavalla.

Tämän lain 1 §:ssä säädettyä tarkoitusta varten kerättyjä henkilötietoja saa käsitellä muuhun kuin 1 §:ssä säädettyyn tarkoitukseen vain, jos käsittelystä säädetään laissa.

Sama tai toinen rekisterinpitäjä saa käsitellä henkilötietoja myös yleisen edun mukaisesti arkistointia taikka tieteellistä, tilastollista tai historiallista käsittelyä varten, edellyttäen että rekisteröidyn oikeuksia koskevat asianmukaiset suojatoimet on toteutettu.

6 §

Tarpeellisuusvaatimus

Käsiteltävien henkilötietojen tulee olla käsittelyn tarkoituksen kannalta asianmukaisia ja tarpeellisia, eivätkä ne saa olla liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään. Tarpeettomat henkilötiedot on poistettava ilman aiheetonta viivytystä.

Henkilötiedot saa säilyttää muodossa, josta rekisteröity on tunnistettavissa vain niin kauan kuin on tarpeen henkilötietojen käsittelyn tarkoituksen kannalta.

Henkilötietojen säilyttämisen tarpeellisuutta on arvioitava vähintään viiden vuoden välein, jollei henkilötietojen säilytysajoista muualla toisin säädetä.

7 §

Virheettömyysvaatimus

Käsiteltävien henkilötietojen tulee olla virheettömiä ja käsittelyn tarkoitus huomioon ottaen päivitettyjä.

8 §

Eräiden henkilötietojen erottaminen toisistaan

Rekisterinpitäjän on erotettava tarvittaessa ja mahdollisuuksien mukaan selvästi toisistaan henkilötiedot, jotka koskevat käsiteltävän asian kannalta eri asemassa olevia rekisteröityjä.

Tosiseikkoihin perustuvien henkilötietojen erottamiseksi henkilökohtaisiin arvioihin perustuvista henkilötiedoista on toteutettava kaikki kohtuulliset toimenpiteet.

9 §

Siirrettävien tai saataville asetettavien henkilötietojen laadun varmentaminen

Toimivaltaisen viranomaisen on toteutettava kaikki kohtuulliset toimenpiteet sen varmistamiseksi, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja siirretä eikä aseteta saataville.

Kaikkiin henkilötietojen siirtoihin on mahdollisuuksien mukaan lisättävä sellaiset tiedot, joiden avulla vastaanottava toimivaltainen viranomainen voi arvioida henkilötietojen paikkansapitävyyttä, täydellisyyttä, luotettavuutta ja ajantasaisuutta.

Jos ilmenee, että on siirretty virheellisiä henkilötietoja tai että henkilötietoja on siirretty lainvastaisesti, on asiasta viipymättä ilmoitettava vastaanottajalle. Vastaanottajan on asiasta tiedon saatuaan oikaistava tai poistettava henkilötiedot tai rajoitettava niiden käsittelyä.

10 §

Ilmoittamisvelvollisuus käsittelyn erityisistä edellytyksistä

Jos henkilötietojen käsittelyyn liittyy laissa säädettyjä erityisiä edellytyksiä, toimivaltaisen viranomaisen on henkilötietojen luovutuksen tai siirron yhteydessä ilmoitettava henkilötietojen vastaanottajalle kyseisistä edellytyksistä sekä velvollisuudesta noudattaa niitä.

Kun toimivaltainen viranomainen siirtää henkilötietoja Euroopan unionissa sijaitsevalle vastaanottajalle, se ei saa asettaa henkilötietojen käsittelylle tiukempia edellytyksiä kuin mitä sovelletaan kansallisesti samankaltaisiin tiedonsiirtoihin.

11 §

Erityisiä henkilötietoryhmiä koskeva käsittely

Erityisiin henkilötietoryhmiin kuuluvia tietoja (*arkaluonteiset henkilötiedot*) ovat henkilötiedot, joista ilmenee etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus taikka ammattiliiton jäsenyys, sekä geneettiset tiedot, luonnollisen henkilön yksiselitteiseen tunnistamiseen tarkoitetut biometriset tiedot tai terveyttä taikka luonnollisen henkilön seksuaalista käyttäytymistä ja seksuaalista suuntautumista koskevat tiedot.

Arkaluonteisten henkilötietojen käsittely on sallittu vain, jos se on välttämätöntä ja edellyttäen, että rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu ja jos:

1. käsittelystä säädetään laissa;
2. rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen sitä edellyttää; tai

3. käsittely koskee tietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi.

12 §

Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä vain, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:

1. toimivaltaisen viranomaisen laissa säädetyn tehtävän suorittamiseksi;
2. rekisteröidyn tai rekisterinpitäjän oikeuksien tai velvollisuuksien toteuttamiseksi; tai
3. 5 §:n 3 momentin mukaista historiallista tai tieteellistä tutkimusta taikka tilastointia varten.

Henkilötunnusta ei saa tarpeettomasti merkitä henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

13 §

Automatisoidut yksittäispäätökset

Sellaisen päätöksen tekeminen, joka perustuu pelkästään automatisoituun henkilötietojen käsittelyyn ja jolla on rekisteröityä koskevia kielteisiä oikeusvaikutuksia tai joka muutoin on hänen kannaltaan merkittävä, on kielletty, jollei laissa toisin säädetä.

3 luku

Rekisterinpitäjä ja henkilötietojen käsittelijä

14 §

Rekisterinpitäjän vastuu

Rekisterinpitäjä vastaa siitä, että henkilötietoja käsitellään lainmukaisesti.

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, jotta se voi varmistaa ja osoittaa, että henkilötietojen käsittely on lainmukaista. Toimenpiteiden toteuttamisessa on otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin kohdistuvat riskit.

15 §

Sisäänrakennettu ja oletusarvoinen tietosuoja

Rekisterinpitäjän tulee sekä henkilötietojen käsittelytapoja määrittäessään että henkilötietojen käsittelyn yhteydessä toteuttaa asianmukaiset tekniset ja organisatoriset suoja-toimenpiteet käsittelyn lainmukaisuuden ja rekisteröidyn oikeuksien suojeleminen varmistamiseksi. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset ratkaisut, toimenpiteiden toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset samoin kuin ne riskit, jotka käsittely henkilön oikeuksille aiheuttaa.

Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet varmistukseksi, että oletusarvoisesti käsitellään vain kunkin erityisen käsittelytarkoituksen kannalta tarpeellisia henkilötietoja.

16 §

Yhteiset rekisterinpitäjät

Jos kaksi tai useampi rekisterinpitäjä määrittää yhdessä käsittelyn tarkoitukset ja keinot, niiden on sovittava keskinäisestä vastuunjaostaan tämän lain mukaisten velvollisuuksien hoitamisessa, jollei vastuunjaosta ole säädetty laissa.

Edellä 1 momentissa tarkoitettujen rekisterinpitäjien on nimettävä keskuudestaan yhteyspisteinä toimiva rekisterinpitäjä, johon rekisteröity voi olla yhteydessä oikeuksiensa käyttöä koskevissa asioissa. Rekisteröity voi kuitenkin aina käyttää tämän lain mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään.

17 §

Henkilötietojen käsittelijä

Henkilötietoja rekisterinpitäjän lukuun käsittelevän on annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä muutoinkin riittävät takeet niistä organisatorisista ja teknisistä toimenpiteistä, joilla se varmistaa, että henkilötietoja käsitellään tässä laissa säädettyjen vaatimusten mukaisesti.

Henkilötietojen käsittelijä ei saa käsitellä henkilötietoja muutoin kuin rekisterinpitäjän ohjeiden mukaisesti, eikä saa siirtää henkilötietojen käsittelyä toiselle käsittelijälle ilman rekisterinpitäjän kirjallista lupaa.

Henkilötietojen käsittelijän suorittamasta henkilötietojen käsittelystä on tehtävä kirjallinen sopimus tai annettava kirjallinen määräys, josta ilmenevät käsiteltävät henkilötiedot, käsittelyn kesto, luonne ja tarkoitus, käsiteltävät henkilötietoryhmät ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. Edellä tarkoitetussa kirjallisessa asiakirjassa on lisäksi määrättävä, että henkilötietojen käsittelijä:

1. toimii ainoastaan rekisterinpitäjän ohjeiden mukaisesti;
2. varmistaa, että henkilötietoja käsittelevät luonnolliset henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai että heitä sitoo lakisääteinen salassapitovelvollisuus;
3. avustaa rekisterinpitäjää kaikin tarkoituksenmukaisin tavoin, jotta voidaan varmistaa, että rekisteröidyn oikeuksia koskevia säännöksiä noudatetaan;
4. rekisterinpitäjän valinnan mukaan poistaa taikka palauttaa tietojenkäsittelypalveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos laissa säädetään henkilötietojen säilyttämisestä;
5. saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tämän pykälän noudattamisen osoittamiseksi;
6. täyttää tässä pykälässä tarkoitetut toisen käsittelijän käyttöä koskevat edellytykset.

18 §

Seloste käsittelytoimista

Rekisterinpitäjän on ylläpidettävä sen vastuulle kuuluvasta henkilötietojen käsittelystä kirjallista selostetta, jossa on seuraavat tiedot:

1. rekisterinpitäjän ja tarvittaessa yhteisen rekisterinpitäjän sekä 38 §:ssä tarkoitetun tietosuojavastaavan nimi ja yhteystiedot;
2. henkilötietojen käsittelyn tarkoitukset ja oikeudellinen peruste;
3. kuvaus rekisteröityjen ryhmästä tai ryhmistä ja käsiteltävistä henkilötietoryhmistä;
4. vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan;
5. kolmanteen maahan tai kansainväliselle järjestölle suoritettujen henkilötietojen siirtojen ryhmät;
6. mahdollisuuksien mukaan eri henkilötietoryhmien poistamisen suunnitellut määräajat;
7. mahdollinen profiloinnin käyttö;
8. mahdollisuuksien mukaan yleinen kuvaus tietojärjestelmistä ja niiden suojauksen periaatteista sekä yleinen kuvaus 31 §:ssä tarkoitetuista teknisistä ja organisatorisista turvatoimista.

Henkilötietojen käsittelijän on ylläpidettävä kaikesta rekisterinpitäjän lukuun suoritettavasta henkilötietojen käsittelystä kirjallista selostetta, jossa on seuraavat tiedot:

1. henkilötietojen käsittelijän tai käsittelijöiden sekä tietosuojavastaavan nimi ja yhteystiedot;
2. kunkin rekisterinpitäjän, jonka lukuun käsittelijä toimii, nimi ja yhteystiedot;
3. kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät;
4. jos rekisterinpitäjä on nimenomaisesti niin ohjeistanut, mahdolliset tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle;
5. mahdollisuuksien mukaan yleinen kuvaus 31 §:ssä tarkoitetuista teknisistä ja organisatorisista turvatoimista.

19 §

Lokitiedot

Rekisterinpitäjän ja henkilötietojen käsittelijän on säilytettävä lokitiedot automaattisessa tietojenkäsittelyjärjestelmässään suoritetusta henkilötietojen keräämisestä, muuttamisesta, kyselystä, luovuttamisesta, siirtämisestä, yhdistämisestä ja poistamisesta. Kyselyjä ja luovutuksia koskevien lokitietojen avulla on pystyttävä selvittämään kyselyn ja luovutuksen peruste, toteutuspäivä ja -aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys.

Lokitietoja saa käyttää ainoastaan käsittelyn lainmukaisuuden tarkistamiseen, sisäiseen valvontaan, henkilötietojen eheyden ja turvallisuuden varmistamiseen sekä rikosoikeudellisiin menettelyihin.

20 §

Tietosuojaa koskeva vaikutustenarviointi

Rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista arvioitava suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojaan.

Jos suunniteltu henkilötietojen käsittely saattaa aiheuttaa merkittävän riskin luonnollisen henkilön oikeuksien toteutumiselle, rekisterinpitäjän on tehtävä kirjallinen vaikutustenarviointi. Vaikutustenarviointiin on sisällytettävä yleinen kuvaus suunnitelluista käsittelytoimista, arvio rekisteröidyn oikeuksiin kohdistuvista riskeistä ja toimet niiden vähentämiseksi sekä toimet, joilla henkilötietojen suoja varmistetaan.

21 §

Valvontaviranomaisen ennakkuuleminen

Rekisterinpitäjän tai henkilötietojen käsittelijän on kuultava Tietosuojavirastoa ennen henkilötietojen käsittelyä, jos:

1. edellä 20 §:n 2 momentissa tarkoitettu kirjallinen vaikutustenarviointi osoittaa, että suunnitelluista suojatoimenpiteistä huolimatta käsittely aiheuttaa merkittävän riskin rekisteröidyn oikeuksille; tai
2. tietojen käsittely muutoin erityisesti uusien tekniikoiden, mekanismien tai menettelyjen käyttämisen johdosta aiheuttaa merkittävän riskin rekisteröityjen oikeuksien kannalta.

Tietosuojavirasto voi laatia luettelon 1 momentissa tarkoitetuista ennakkuulemistä edellyttävistä käsittelytoimenpiteistä.

Rekisterinpitäjän on toimitettava Tietosuojavirastolle kirjallinen vaikutustenarviointi ja pyynnöstä muut sellaiset tiedot, joiden avulla virasto voi arvioida henkilötietojen käsittelyn lainmukaisuutta.

Jos Tietosuojavirasto katsoo, että 1 momentissa tarkoitettu käsittely muodostuisi tämän lain vastaiseksi, viraston tulee antaa kuuden viikon kuluessa kuulemispyynnön vastaanottamisesta rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle ohjausta käsittelyn saattamiseksi lainmukaiseksi. Määräaikaa voidaan jatkaa kuukaudella, jos suunnitellun käsittelyn monimutkaisuus sitä edellyttää. Tietosuojaviraston on ilmoitettava rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle määräajan jatkamisesta sekä viivästymisen syistä kuukauden kuluessa kuulemispyynnön vastaanottamisesta.

4 luku

Rekisteröidyn oikeudet

22 §

Yleisesti saataville asetettava tietosuojaseloste

Rekisterinpitäjän on ylläpidettävä sen vastuulle kuuluvasta henkilötietojen käsittelystä kirjallista selostetta, joka on julkistettava ja jossa on ainakin seuraavat tiedot:

1. rekisterinpitäjän ja tietosuojavastaavan yhteystiedot sekä, jos se katsotaan tarpeelliseksi, tietosuojavastaavan nimi;
2. yhteisten rekisterinpitäjien yhteyspisteenä toimivan rekisterinpitäjän nimi ja yhteystiedot sekä tieto siitä, että rekisteröity voi käyttää tämän lain mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään;
3. henkilötietojen käsittelyn tarkoitukset ja oikeusperuste;
4. henkilötietojen säilytysaika, tai jos sitä ei ole määritetty, säilytysajan määrittämiskriteerit;
5. mahdolliset henkilötietojen säännönmukaiset vastaanottajat tai vastaanottajaryhmät,
6. tieto siitä, että rekisteröidyllä on oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten henkilötietojen oikaisemista, poistamista tai niiden käsittelyn rajoittamista;
7. tieto siitä, että rekisteröidyllä on oikeus tehdä 55 §:ssä tarkoitettu kantelu Tietosuojavirastolle, ja viraston yhteystiedot; ja
8. mahdolliset muut rekisteröidyn oikeuksien käyttämiseksi tarpeelliset tiedot.

23 §

Rekisteröidyn tarkastusoikeus

Jokaisella on oikeus saada rekisterinpitäjältä tieto siitä, käsitelläänkö häntä koskevia henkilötietoja. Jos kyseisiä tietoja käsitellään, rekisteröidyllä on oikeus saada rekisterinpitäjältä seuraavat tiedot:

1. käsiteltävät henkilötiedot ja kaikki tietojen alkuperästä käytettävissä olevat tiedot;
2. käsittelyn tarkoitukset ja oikeusperuste;
3. käsittelyn kohteena olevat henkilötietoryhmät;
4. vastaanottajat tai vastaanottajaryhmät, joille rekisteröidyn henkilötietoja on luovutettu;
5. henkilötietojen säilytysaika, tai jos sitä ei ole määritetty, säilytysajan määrittämiskriteerit;
6. rekisteröidyn oikeus pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista, poistamista tai niiden käsittelyn rajoittamista; ja
7. rekisteröidyn oikeus tehdä 55 §:ssä tarkoitettu kantelu Tietosuojavirastolle ja viraston yhteystiedot.

Se, joka haluaa tarkastaa itseään koskevat tiedot 1 momentissa tarkoitettulla tavalla, voi esittää tätä tarkoittavan pyynnön rekisterinpitäjälle omakätisesti allekirjoitetulla asiakirjalla tai sitä vastaavalla varmennetulla tavalla tai henkilökohtaisesti rekisterinpitäjän luona.

24 §

Tarkastusoikeuden rajoitukset

Rekisteröidyn tarkastusoikeutta voidaan lykätä tai rajoittaa tai se voidaan evätä 28 §:ssä säädetyillä perusteilla. Jos rekisteröidyn tarkastusoikeutta lykätään, rajoitetaan tai se evätään, rekisterinpitäjän on ilman aiheetonta viivytystä ilmoitettava siitä kirjallisesti rekisteröidylle. Myös lykkäämisen, rajoittamisen tai epäämisen perustelut on ilmoitettava, paitsi jos niiden ilmoittaminen vaarantaisi epäämisen tai rajoittamisen tarkoituksen. Tarkastusoikeuden epäämisen veroisena pidetään sitä, että rekisterinpitäjä ei ole kolmen kuukauden kuluessa pyynnön esittämisestä antanut kirjallista vastausta rekisteröidylle.

Rekisterinpitäjän on ilmoitettava rekisteröidylle tämän oikeudesta tehdä kantelu Tietosuojavirastolle ja käyttää oikeussuojakeinoja tarkastusoikeuden lykkäämisen, rajoittamisen tai epäämisen johdosta, samoin kuin mahdollisesta oikeudesta käyttää tarkastusoikeutta 29 §:n mukaisesti Tietosuojaviraston välityksellä.

Rekisterinpitäjän on säilytettävä tieto niistä perusteista, joihin tarkastusoikeuden epääminen tai rajoittaminen perustuu.

25 §

Henkilötietojen oikaiseminen, poistaminen tai käsittelyn rajoittaminen

Rekisterinpitäjän on oma-aloitteisesti tai rekisteröidyn vaatimuksesta ilman aiheetonta viivytystä oikaistava tai täydennettävä rekisteröityä koskeva, käsittelyn tarkoituksen kannalta virheellinen tai puutteellinen henkilötieto.

Rekisterinpitäjän on oma-aloitteisesti tai rekisteröidyn vaatimuksesta ilman aiheetonta viivytystä poistettava rekisteröityä koskevat henkilötiedot, jos niiden käsittely on vastoin 4–7 tai 11 §:ssä säädettyä. Poistamisen sijasta rekisterinpitäjän on kuitenkin rajoitettava käsittelyä, jos

1. rekisteröity kiistää tietojen paikkansapitävyyden eikä niiden paikkansapitävyyttä tai virheellisyyttä voida todentaa; tai
2. henkilötiedot on säilytettävä todistelua varten.

Jos käsittelyä on rajoitettu 2 momentin 1 kohdan nojalla, rekisterinpitäjän on ennen rajoituksen poistamista ilmoitettava siitä rekisteröidylle.

26 §

Rekisteröidyn vaatimuksen epääminen

Jollei rekisterinpitäjä hyväksy rekisteröidyn vaatimusta henkilötietojen oikaisemisesta, täydentämisestä, poistamisesta tai niiden käsittelyn rajoittamisesta, rekisterinpitäjän on ilmoitettava rekisteröidylle kirjallisesti kieltäytymisestä ja sen syistä. Tiedot kieltäytymisen perusteista voidaan kokonaan tai osittain jättää antamatta siltä osin kuin se on välttämätöntä 28 §:ssä säädettyistä syistä.

Rekisterinpitäjän on ilmoitettava rekisteröidylle tämän oikeudesta kannella Tietosuoja-
virastolle ja viraston yhteystiedot, mahdollisesta oikeudesta käyttää 25 §:ssä tarkoitettuja oikeuksia 29 §:n mukaisesti Tietosuojaviraston välityksellä sekä tämän mahdollisuudesta käyttää muita oikeussuojakeinoja.

27 §

Rekisterinpitäjän velvollisuus ilmoittaa oikaisemisesta, poistamisesta tai käsittelyn rajoittamisesta

Rekisterinpitäjän on ilmoitettava virheellisten henkilötietojen oikaisemisesta sille viranomaiselle, jolta virheelliset henkilötiedot ovat peräisin.

Jos henkilötietoja on oikaistu tai poistettu taikka niiden käsittelyä on rajoitettu, rekisterinpitäjän on ilmoitettava asiasta niille vastaanottajille, joille rekisterinpitäjä on luovuttanut kyseisiä tietoja.

28 §

Rekisteröidyn oikeuksien rajoittaminen

Rekisteröidyn oikeuksia voidaan rajoittaa 24 §:n 1 momentissa, 26 §:n 1 momentissa ja 35 §:ssä tarkoitetulla tavalla, jos se rekisteröidyn oikeudet huomioon ottaen on oikeasuhtaista ja välttämätöntä:

1. jotta vältetään tuottamasta haittaa rikosten ennalta estämiselle, paljastamiselle, selvittämiseksi tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle;
2. viranomaisen muun tutkinnan, selvityksen tai vastaavan menettelyn turvaamiseksi;
3. yleisen turvallisuuden suojelemiseksi;

4. kansallisen turvallisuuden suojelemiseksi; tai
5. muiden henkilöiden oikeuksien suojaamiseksi.

29 §

Oikeuksien käyttäminen Tietosuojaviraston välityksellä

Rekisteröidyllä on oikeus pyytää Tietosuojavirastoa tarkastamaan henkilötietojen ja niiden käsittelyn lainmukaisuus, jos tämän tai muun lain nojalla rekisteröidyn tarkastusoikeutta on lykätty, rajoitettu tai evätty tai jos rekisterinpitäjä ei hyväksy rekisteröidyn vaatimusta henkilötietojen oikaisemisesta, täydentämisestä, poistamisesta tai rajoittamisesta.

Jos rekisteröity käyttää 1 momentissa tarkoitettua oikeuttaan, Tietosuojaviraston on kohtuullisen ajan kuluessa ilmoitettava rekisteröidylle toimenpiteistä, joihin se on ryhtynyt. Tietosuojaviraston on myös ilmoitettava rekisteröidylle hänen oikeudestaan käyttää oikeussuojakeinoja.

30 §

Rekisteröidyn oikeuksien käytön edistäminen ja toimenpiteiden maksuttomuus

Rekisterinpitäjän on edistettävä rekisteröityjen mahdollisuuksia käyttää tässä luvussa tarkoitettuja oikeuksia. Kaikki rekisteröidylle annettavat ilmoitukset ja henkilötietojen käsittelyä koskevat tiedot on annettava tiiviisti esitetyssä, ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.

Rekisteröidylle tämän lain mukaisesti annettavat ilmoitukset ja tiedot sekä rekisteröidyn tämän lain mukaisesti tekemien pyyntöjen käsitteleminen ovat rekisteröidylle maksuttomia. Jos rekisteröidyn pyynnöt ovat niiden toistuvuudesta tai muusta syystä ilmeisen kohtuuttomia tai perusteettomia, rekisterinpitäjä voi kuitenkin periä toimenpiteestä maksun siten kuin valtion maksuperustelaisissa (150/1992) säädetään.

Jos rekisterinpitäjä 2 momentissa tarkoitettulla tavalla perii maksun, sen on tarvittaessa osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

5 luku

Tietoturvallisuus

31 §

Henkilötietojen suojaaminen

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee teknisin ja organisatorisin toimenpitein suojata henkilötiedot varmistaakseen sellaisen tietoturvallisuuden tason, jota käsittelystä rekisteröidyn oikeuksille aiheutuvan riskin voidaan katsoa edellyttävän. Henkilötiedot on erityisesti suojattava oikeudettomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta. Toimenpiteitä suunniteltaessa ja toteutettaessa tulee ottaa huomioon:

1. uusin tekniikka;
2. toimenpiteiden toteuttamiskustannukset;
3. käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset; ja
4. luonnollisen henkilön oikeuksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

32 §

Henkilötietojen suojaaminen automatisoidussa käsittelyssä

Automatisoidun käsittelyn osalta rekisterinpitäjän tai henkilötietojen käsittelijän on 31 §:ssä edellytetyn lisäksi toteutettava riskien arvioinnin pohjalta toimenpiteet, joiden tarkoituksena on:

1. evätä asiattomilta pääsy käsittelyyn käytettäviin laitteisiin;
2. estää tietovälineiden luvaton lukeminen, jäljentäminen, muuttaminen tai poistaminen;
3. estää henkilötietojen luvaton syöttäminen järjestelmään sekä järjestelmään tallennettujen henkilötietojen luvaton tarkastelu, muuttaminen tai poistaminen;
4. estää asiattomia käyttämästä automatisoituja käsittelyjärjestelmiä tiedonsiirtolaitteiden avulla;
5. varmistaa, että automatisoidun käsittelyjärjestelmän käyttöön oikeutetut henkilöt pääsevät ainoastaan käyttöoikeuksiensa piiriin kuuluviin henkilötietoihin;
6. varmistaa, että on mahdollista tarkistaa ja todeta, mille tahoille henkilötietoja on siirretty tai asetettu saataville tai voidaan siirtää tai asettaa saataville tiedonsiirtolaitteiden avulla;

7. varmistaa, että jälkikäteen on mahdollista tarkistaa ja todeta, mitä henkilötietoja on syötetty automatisoituihin käsittelyjärjestelmiin, milloin niitä on syötetty ja kuka niitä on syöttänyt;
8. estää henkilötietojen oikeudeton lukeminen, jäljentäminen, muuttaminen tai poistaminen tietoja siirrettäessä tai tietovälineitä kuljetettaessa;
9. varmistaa, että käytetyt järjestelmät voidaan häiriön tapahtuessa palauttaa entiselleen;
10. varmistaa, että järjestelmä toimii, että havaituista toimintojen virheistä ilmoitetaan ja että järjestelmän toimintahäiriö ei voi vahingoittaa tallennettuja henkilötietoja.

33 §

Henkilötietojen käsittelijän velvollisuus ilmoittaa tietoturvaloukkauksesta

Henkilötietojen käsittelijän on henkilötietojen tietoturvaloukkauksesta tiedon saatuaan ilman aiheetonta viivytystä ilmoitettava loukkauksesta rekisterinpitäjälle.

34 §

Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta Tietosuojavirastolle

Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta Tietosuojavirastolle, paitsi jos loukkauksesta ei todennäköisesti aiheudu vaaraa rekisteröidyn oikeuksille.

Rekisterinpitäjän on tehtävä ilmoitus ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa saatuaan tietoturvaloukkauksen tietoonsa. Jos ilmoitus Tietosuojavirastolle tehdään tätä myöhemmin, ilmoituksessa on kerrottava viivytyksen syyt.

Rekisterinpitäjän on säilytettävä tiedot tietoturvaloukkauksista ja niihin liittyvistä seikoista, niiden vaikutuksista ja toteutetuista korjaavista toimenpiteistä.

35 §

Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta rekisteröidylle

Rekisterinpitäjän on ilman aiheetonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisteröidylle, jos tietoturvaloukkaus todennäköisesti aiheuttaa merkittävän riskin rekisteröidyn oikeuksille. Ilmoittamisvelvollisuutta ei kuitenkaan ole, jos:

1. loukkauksen kohteena oleviin henkilötietoihin on sovellettu asianmukaisia teknisiä ja organisatorisia suojaustoimenpiteitä; tai
2. rekisterinpitäjä on loukkauksen jälkeen ryhtynyt toimenpiteisiin sen varmistamiseksi, ettei rekisteröidyn oikeuksiin kohdistuva riski todennäköisesti toteudu.

Rekisterinpitäjä voi rekisteröidylle tehtävän ilmoituksen sijasta tiedottaa tietoturvaloukkauksesta julkisella ilmoituksella, jos ilmoituksen tekeminen rekisteröidylle vaatisi kohtuutonta vaivaa.

Rekisteröidylle ilmoittamista voidaan lykätä tai rajoittaa tai se voidaan jättää tekemättä, jos 28 §:ssä säädetty edellytykset täyttyvät.

36 §

Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta toiselle rekisterinpitäjälle

Rekisterinpitäjän on ilman aiheetonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta sellaiselle Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle, jonka toimittamiin tai jolle toimitettuihin tietoihin loukkaus kohdistuu.

37 §

Tietoturvaloukkauksesta annettavan ilmoituksen sisältö

Tietosuojavirastolle ja Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle annettavassa ilmoituksessa on kuvattava henkilötietojen tietoturvaloukkaus. Kuvaukseen on mahdollisuuksien mukaan sisällytettävä tiedot asianomaisten rekisteröityjen ryhmistä, rekisteröityjen arvioidusta lukumäärästä, henkilötietotyyppien ryhmistä ja henkilötietojen arvioidusta lukumäärästä.

Rekisteröidylle annettavassa ilmoituksessa on kuvattava tietoturvaloukkauksen luonne.

Edellä 1 ja 2 momentissa tarkoitetuista ilmoituksista on lisäksi käytävä ilmi:

1. tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;
2. tietoturvaloukkauksen todennäköiset seuraukset; ja
3. toimenpiteet, jotka rekisterinpitäjä on toteuttanut tai joita se on ehdottanut tietoturvaloukkauksen johdosta ja tarvittaessa toimenpiteet sen haittavaikutusten lieventämiseksi.

Tietosuojavirastolle ja Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle annettavat tiedot voidaan toimittaa vaiheittain siltä osin kuin niitä ei ole mahdollista toimittaa samanaikaisesti.

6 luku

Tietosuojavastaava

38 §

Tietosuojavastaavan nimeäminen

Rekisterinpitäjän on nimettävä tietosuojavastaava, jolla on riittävä asiantuntemus henkilötietojen käsittelyä koskevasta lainsäädännöstä ja alan käytänteistä sekä valmiudet hoitaa 40 §:ssä tarkoitetut tehtävät. Yksi tietosuojavastaava voidaan nimetä useaa toimivaltaista viranomaista varten, jos se on perusteltua viranomaisten organisaatorakenne ja koko huomioon ottaen.

Rekisterinpitäjän on ilmoitettava tietosuojavastaavan yhteystiedot Tietosuojavirastolle.

39 §

Tietosuojavastaavan asema

Rekisterinpitäjän on otettava tietosuojavastaava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn.

Rekisterinpitäjän on turvattava tietosuojavastaavan toimintaedellytykset tälle 40 §:ssä säädettyjen tehtävien hoitamiseksi sekä annettava pääsy henkilötietoihin ja käsittelytoimiin.

40 §

Tietosuojavastaavan tehtävät

Tietosuojavastaavan tehtävänä on:

1. neuvoa rekisterinpitäjää ja henkilötietoja sen palveluksessa käsitteleviä henkilötietojen suojaa koskevissa asioissa;
2. valvoa henkilötietojen käsittelyä koskevan sääntelyn ja rekisterinpitäjän henkilötietojen käsittelyyn liittyvien menettelytapojen noudattamista;

3. antaa pyydettyä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa, että se toteutetaan 20 §:ssä säädetyn mukaisesti;
4. tehdä yhteistyötä Tietosuojaviraston kanssa ja toimia sen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tietosuojavastaavan tehtävät eivät koske tuomioistuinten, valtioneuvoston oikeuskanslerin eikä eduskunnan oikeusasiamiehen lainkäyttötehtävien yhteydessä suorittamaa henkilötietojen käsittelyä.

7 luku

Henkilötietojen siirrot kolmansiin maihin ja kansainvälisille järjestöille

41 §

Henkilötietojen siirtoja koskevat yleiset periaatteet

Toimivaltainen viranomainen saa siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos tässä laissa tarkoitettuun henkilötietojen käsittelyyn sovellettavia muita säännöksiä noudatetaan ja jos:

1. siirto on tarpeen tämän lain 1 §:n 1 momentissa mainittua tarkoitusta varten;
2. henkilötiedot siirretään kolmannen maan rekisterinpitäjälle tai kansainväliselle järjestölle, joka on toimivaltainen käsittelemään henkilötietoja 1 §:n 1 momentissa mainitussa tarkoituksessa; ja
3. tietosuojan riittävydestä on tietosuojadirektiivin 36 artiklassa tarkoitettu Euroopan komission (*komissio*) voimassaoleva päätös tai jollei tällaista päätöstä ole tehty, asianmukaiset suojatoimet ovat olemassa 42 §:n mukaisesti, tai 43 §:ssä säädetty erityistilanteita koskevat poikkeukset tulevat sovellettaviksi.

Jos henkilötiedot on saatu toisesta EU:n jäsenvaltiosta, siirron edellytyksenä on lisäksi, että kyseinen jäsenvaltio on antanut siirrolle luvan. Siirto, joka tehdään ilman tällaista lupaa, on sallittu vain, jos se on välttämätön jonkin maan yleiseen turvallisuuteen tai EU:n jäsenvaltion olennaisiin etuihin kohdistuvan välittömän ja vakavan uhan estämiseksi, eikä lupaa voida saada ajoissa. Siirrosta on ilmoitettava viipymättä ennakkoluvan antamisesta vastaavalle viranomaiselle.

Jos henkilötiedot siirretään edelleen muuhun kolmanteen maahan tai muulle kansainväliselle järjestölle, alkuperäisen siirron toteuttanut toimivaltainen viranomainen voi antaa luvan edelleen siirtämiselle noudattaen, mitä 1 ja 2 momentissa säädetään ja ottaen asianmukaisesti huomioon kaikki merkittävät seikat, kuten rikoksen vakavuus, henkilötietojen alkuperäisen siirron tarkoitus ja henkilötietojen suojan taso siinä kol-

mannessa maassa tai kansainvälisessä järjestössä, johon tai jolle tiedot siirretään edelleen.

42 §

Siirto asianmukaisten suojatoimien perusteella

Jos komissio ei ole tehnyt 41 §:n 1 momentin 3 kohdassa tarkoitettua päätöstä, henkilötietoja voidaan siirtää kolmanteen maahan tai kansainväliselle järjestölle, jos muut 41 §:ssä säädetty edellytykset täyttyvät, ja:

1. oikeudellisesti sitovassa asiakirjassa määrätään asianmukaisista henkilötietojen suojatoimista; tai
2. rekisterinpitäjä kaikkia henkilötietojen siirtoon liittyviä seikkoja arvioituaan katsoo, että henkilötietojen suojaamiseksi on toteutettu asianmukaiset suojatoimet.

Rekisterinpitäjän on ilmoitettava Tietosuojavirastolle 1 momentin 2 kohdan perusteella tehtyjen siirtojen sarjat. Tiedot kyseisistä siirroista on säilytettävä ja ne on asetettava pyynnöstä Tietosuojaviraston saataville. Säilytettäviin tietoihin tulee kuulua tiedot siirtojen päivämääristä ja ajankohdista, vastaanottavasta toimivaltaisesta viranomaisesta, siirtojen perusteista ja siirretyistä henkilötiedoista.

43 §

Erityistilanteita koskevat poikkeukset

Jos komissio ei ole tehnyt 41 §:n 1 momentin 3 kohdassa tarkoitettua päätöstä eikä 42 §:ssä säädetty tiedonsiirron edellytykset täyty, voidaan henkilötietoja siirtää kolmanteen maahan tai kansainväliselle järjestölle vain, jos siirto on tarpeen:

1. rekisteröidyn tai toisen henkilön elintärkeiden etujen suojaamiseksi;
2. rekisteröidyn oikeutettujen etujen turvaamiseksi;
3. EU:n jäsenvaltion tai kolmannen maan yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhkan estämiseksi; tai
4. yksittäistapauksessa 1 §:n 1 momentissa mainittuja tarkoituksia varten tai niihin liittyvien oikeusvaateiden laatimiseksi, esittämiseksi tai puolustamiseksi.

Henkilötietoja ei kuitenkaan saa siirtää 1 momentin 4 kohdan nojalla, jos asianomaisen rekisteröidyn oikeuksia on pidettävä siirtoa puoltavaa yleistä etua painavampana.

Tiedot siirroista, jotka perustuvat 1 momenttiin, on säilytettävä ja ne on asetettava pyynnöstä Tietosuojaviraston saataville. Säilytettäviin tietoihin kuuluvat tiedot siirron päivämäärästä ja ajankohdasta, vastaanottavasta toimivaltaisesta viranomaisesta, siirron perusteista ja siirretyistä henkilötiedoista.

44 §

Henkilötietojen siirto kolmansiin maihin yksityisille ja muille vastaanottajille

Edellä 3 §:n 7 kohdan a alakohdassa tarkoitettu toimivaltainen viranomainen voi yksittäisessä tapauksessa 41 §:n 1 momentin 2 kohdassa säädetyn estämättä siirtää henkilötietoja suoraan kolmansiin maihin sijoittautuneille yksityisille ja muille vastaanottajille, jos tämän lain muita säännöksiä noudatetaan ja jos:

1. siirto on välttämätön, jotta siirron toteuttava toimivaltainen viranomainen voi suorittaa sille säädetty 1 §:n 1 momentissa tarkoitetut tehtävänsä;
2. tietoja siirtävä toimivaltainen viranomainen katsoo, että asianomaisen rekisteröidyn oikeudet eivät syrjäytä yleistä etua, jonka perusteella siirto käsiteltävänä olevassa tapauksessa on tarpeen;
3. tietoja siirtävä toimivaltainen viranomainen katsoo, että siirto kolmannen maan toimivaltaiselle viranomaiselle olisi asian kiireellisyydestä tai muusta syystä tehoton tai epätarkoituksenmukainen;
4. kolmannen maan viranomaiselle, joka on toimivaltainen 1 §:n 1 momentin mukaisissa tarkoituksissa, ilmoitetaan siirrosta ilman aiheutonta viivästystä, ellei tämä ole tehotonta tai epätarkoituksenmukaista;
5. tietoja siirtävä toimivaltainen viranomainen ilmoittaa vastaanottajalle, mitä tiettyä tarkoitusta tai tiettyjä tarkoituksia varten tämä saa käsitellä henkilötietoja, että käsittelyn on oltava tarpeellista näitä tarkoituksia varten, ja että tietoja ei saa käsitellä muita tarkoituksia varten, ja
6. siirto ei ole vastoin Suomen kansainvälisiä sopimusvelvoitteita.

Tiedot siirtävän toimivaltaisen viranomaisen on säilytettävä tiedot 1 momentin nojalla tehtävästä siirrosta ja ilmoitettava siirrosta Tietosuojavirastolle.

8 luku

Valvontaviranomainen

45 §

Tietosuojavirasto

Tämän lain noudattamista valvoo tietosuojalain (___201_) 7 §:ssä tarkoitettu Tietosuojavirasto.

Tämän luvun säännöksiä valvonnasta ei sovelleta tuomioistuinten, valtioneuvoston oikeuskanslerin eikä eduskunnan oikeusasiamiehen lainkäyttöön liittyvään toimintaan.

Tietosuojavirasto toimii riippumattomasti hoitaessaan tässä laissa säädettyjä tehtäviään.

46 §

Tehtävät

Tietosuojaviraston tehtäviin kuuluu tämän lain noudattamisen valvomisen lisäksi:

1. edistää yleistä tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, lain-säädännöstä, suojatoimista ja oikeuksista;
2. edistää rekisterinpitäjien ja henkilötietojen käsittelijöiden tietoisuutta niille tämän lain mukaan kuuluvista velvollisuuksista;
3. antaa pyynnöstä rekisteröidyille tietoja heille tämän lain nojalla kuuluvien oikeuksien käyttämisestä;
4. antaa neuvontaa 21 §:ssä tarkoitetussa ennakkokuulemisessa;
5. tehdä selvityksiä tämän lain noudattamisesta;
6. tarkistaa 29 §:n mukaisesti käsittelyn lainmukaisuus;
7. käsitellä rekisteröidyn tai 55 §:n 2 momentissa tarkoitetun yhteisön tekemiä; ja
8. seurata henkilötietojen suojaan vaikuttavaa teknologista ja muuta kehitystä.

Tietosuojaviraston tehtävänä on lisäksi osallistua asetuksella (EU) 2016/679 perustetun tietosuojaneuvoston toimintaan. Tietosuojavirasto ei kuitenkaan vie neuvoston käsiteltäväksi asiaa, jossa on kyse henkilötietojen käsittelystä 1 §:n 2 momentissa tarkoitetun toiminnan yhteydessä.

Tietosuojaviraston toimenpiteet ovat rekisteröidylle ja tietosuojavastaavalle maksuttomia. Jos rekisteröidyn tai tietosuojavastaavan pyynnöt kuitenkin ovat pyyntöjen toistuvuudesta tai muusta syystä ilmeisen kohtuuttomia tai perusteettomia, virasto voi:

1. periä toimenpiteistä maksun siten kuin valtion maksuperustelaissa (150/1992) säädetään; tai
2. jättää pyynnön kohteena olevan asian tutkimatta.

Jos Tietosuojavirasto 2 momentissa tarkoitetulla tavalla perii maksun tai jättää asian tutkimatta, sen on tarvittaessa osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

47 §

Tietojensaantioikeus

Tietosuojavirastolla on oikeus salassapitosäännösten estämättä saada rekisterinpitäjältä ja henkilötietojen käsittelijältä sekä tämän edustajalta maksutta 22 §:ssä tarkoitettu seloste käsittelytoimista, 19 §:ssä tarkoitetut lokitiedot sekä muut tehtäviensä hoitamiseksi välttämättömät tiedot.

Tietosuojavirastolla on oikeus saada rekisterinpitäjältä ja henkilötietojen käsittelijältä selvitys seikoista, jotka ovat tarpeen viraston tehtävien hoitamiseksi.

48 §

Oikeus tehdä tarkastuksia

Tietosuojavirasto voi tehdä tarkastuksen rekisterinpitäjän ja henkilötietojen käsittelijän toimitiloissa, jos tarkastus on tarpeen tämän lain noudattamisen valvomiseksi. Tarkastusta ei saa tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa. Tarkastuksessa noudatetaan, mitä hallintolain (434/2003) 39 §:ssä säädetään.

Poliisi on velvollinen tarvittaessa antamaan Tietosuojavirastolle virka-apua 1 momentissa tarkoitetun tarkastuksen suorittamiseksi.

49 §

Asiantuntijan käyttö

Tietosuojavirasto voi 48 §:ssä tarkoitetun tarkastuksen yhteydessä käyttää apunaan ulkopuolista asiantuntijaa. Tietosuojavirasto voi nimetä asiantuntijaksi suostumuksensa tehtävään antaneen henkilön, jolla on Tietosuojaviraston tehtävän hoitamisen kannalta merkityksellistä asiantuntemusta.

Edellä 1 momentissa tarkoitettuun asiantuntijaan sovelletaan virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä.

50 §

Toimenpiteet

Tietosuojavirasto voi tämän lain soveltamisalalla:

1. antaa rekisterinpitäjälle ohjausta 21 §:ssä tarkoitetussa ennakkokuulemismenettelyssä;
2. ilmoittaa rekisterinpitäjälle tai henkilötietojen käsittelijälle tämän lain väitetystä rikkomisesta;
3. varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää siitä, että aiotut käsittelytoimet voivat olla tämän lain vastaisia;
4. antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos tämä on käsitellyt henkilötietoja lainvastaisesti;
5. määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat rekisteröidyn tähän lakiin perustuvien oikeuksien käyttöä;
6. määrätä rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle;
7. asettaa väliaikaisen tai pysyvän kiellon tai muun rajoituksen käsittelylle;
8. määrätä tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle;
9. määrätä henkilötietojen oikaisemisesta tai poistamisesta tai käsittelyn rajoittamisesta tai niihin liittyvistä muista toimenpiteistä 25 §:n perusteella;
10. määrätä rekisterinpitäjän tai henkilötietojen käsittelijän saattamaan käsittelytoimet tämän lain säännösten mukaisiksi, tarvittaessa määrättyllä tavalla ja kohtuullisen määräajan kuluessa.

51 §

Uhkasakko

Tietosuojavirasto voi asettaa 50 §:n 5–10 kohdassa tarkoitetun päätöksen ja 47 §:ssä tarkoitetun tiedonsaantioikeuden tehosteeksi uhkasakon. Uhkasakon asettamisesta ja tuomitsemisesta maksettavaksi säädetään uhkasakkolaissa (1113/1990).

52 §

Tietosuojaviraston kuuleminen

Tietosuojavirasto voi omasta aloitteestaan tai pyynnöstä antaa lausuntoja 1 §:ssä tarkoitettuun henkilötietojen käsittelyyn liittyvistä kysymyksistä.

Tietosuojavirastolle on varattava tilaisuus tulla kuulluksi valmisteltaessa 1 §:ssä tarkoitettua henkilötietojen käsittelyä koskevia lainsäädännöllisiä tai hallinnollisia uudistuksia.

Tuomioistuimen on sen käsiteltävänä olevassa, tämän lain soveltamista koskevassa asiassa varattava Tietosuojavirastolle mahdollisuus tulla kuulluksi. Syyttäjän on varattava Tietosuojavirastolle mahdollisuus tulla kuulluksi tämän lain vastaista menettelyä koskevissa asioissa.

53 §

Keskinäinen avunanto

Tietosuojaviraston on maksutta annettava toisen EU:n jäsenvaltion vastaavalle valvontaviranomaiselle tämän valvontatehtävässään välttämättä tarvitsemat henkilötiedot sekä muut tarpeelliset tiedot, ja tarvittaessa muutoinkin avustettava tätä valvonnan toteuttamisessa. Tietosuojaviraston on ryhdyttävä muihinkin tarvittaviin toimenpiteisiin tehokkaan keskinäisen yhteistyön varmistamiseksi.

Tietosuojaviraston on vastattava 1 momentissa tarkoitetun valvontaviranomaisen esittämään pyyntöön ilman aiheetonta viivytystä ja joka tapauksessa viimeistään kuukauden kuluttua pyynnön vastaanottamisesta.

9 luku

Oikeusturva

54 §

Rikkomisista ilmoittaminen

Toimivaltaisella viranomaisella on oltava menettelytavat, joita noudattamalla sille voidaan luottamuksellisesti ilmoittaa tämän lain epäilystä rikkomisesta. Ilmoitusmenettelyn tulee sisältää asianmukaiset ja riittävät toimenpiteet, joilla järjestetään ilmoitusten asianmukainen käsittely. Ilmoitusmenettelyn tulee lisäksi sisältää ohjeet, joilla turvataan ilmoituksen tekijän henkilöllisyyden suoja.

Toimivaltaisen viranomaisen on säilytettävä 1 momentissa tarkoitettua ilmoitusta koskevat tarpeelliset tiedot. Tiedot on poistettava viiden vuoden kuluttua ilmoituksen tekemisestä, jollei tietojen edelleen säilyttäminen ole tarpeen rikostutkinnan, vireillä olevan oikeudenkäynnin, viranomaistutkinnan taikka ilmoituksen tekijän tai ilmoituksen kohteena olevan henkilön oikeuksien turvaamiseksi. Tietojen edelleen säilyttämisen tarpeellisuus on tutkittava viimeistään kolmen vuoden kuluttua edellisestä tarkistamisesta. Tarkistamisesta on tehtävä merkintä.

Kun luonnollinen henkilö on tehnyt toimivaltaiselle viranomaiselle ilmoituksen tämän lain epäilystä rikkomisesta, ilmoittajan henkilöllisyys on pidettävä salassa, jos henkilöllisyyden paljastamisesta voidaan olosuhteiden perusteella arvioida aiheutuvan haittaa ilmoittajalle.

Edellä 3 momentissa tarkoitettussa tilanteessa ei sovelleta viranomaisten toiminnan julkisuudesta annetun lain säännöksiä asianosaisen oikeudesta tiedonsaantiin, jos ilmoittajan henkilöllisyyden ilmaiseminen vaarantaisi hänen turvallisuuttaan, etujaan tai oikeuksiaan.

55 §

Kantelu Tietosuojavirastolle

Rekisteröidyllä on oikeus kannella Tietosuojavirastolle, jos rekisteröity katsoo, että häneen liittyvässä henkilötietojen käsittelyssä rikotaan tätä lakia.

Kantelun voi rekisteröidyn suostumuksella saattaa Tietosuojaviraston käsiteltäväksi myös yleishyödyllinen henkilötietojen suoja edistävä yhteisö.

56 §

Kantelun käsitteleminen

Tietosuojavirasto tutkii kantelun sekä ilmoittaa sen tekijälle asian käsittelyn etenemisestä ja sen tuloksista kohtuullisen ajan kuluessa. Virasto ei kuitenkaan ota tutkittavaksi tuomioistuimessa vireillä olevaa asiaa.

Jos Tietosuojavirasto pitää sillä vireillä olevassa, tämän lain noudattamisen valvontaa koskevassa asiassa tarpeellisenä selvittää, onko Euroopan komission 41 §:n 1 momentin 3 kohdassa tarkoitettu päätös tietosuojan tason riittävydestä tietosuojadirektiivin mukainen, virasto voi hakemuksella saattaa valvontaa koskevan asian Helsingin hallinto-oikeuden ratkaistavaksi.

57 §

Muutoksenhaku

Tietosuojaviraston tekemään päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen sen mukaan kuin hallintolainkäyttölaissa (586/1996) säädetään.

Hallinto-oikeuden päätökseen 56 §:n 2 momentissa tarkoitettussa asiassa saa hakea muutosta valittamalla korkeimpaan hallinto-oikeuteen siten kuin hallintolainkäyttölaissa säädetään.

Muuhun hallinto-oikeuden päätökseen saa hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan. Myös Tietosuojavirasto saa hakea muutosta tällaiseen hallinto-oikeuden päätökseen.

Tietosuojaviraston päätöksessä voidaan määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei valitusviranomainen toisin määrää.

10 luku

Erinäiset säännökset

58 §

Vahingonkorvaus

Rekisterinpitäjä on velvollinen korvaamaan sen taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle tämän lain vastaisesta henkilötietojen käsittelystä.

Muutoin oikeudesta saada korvaus vahingosta säädetään vahingonkorvauslaissa (412/1974).

59 §

Rikoslain rangaistussäännökset

Rangaistus Tietosuoja-rikoksesta säädetään rikoslain (39/1889) 38 luvun 9 §:ssä. Rangaistus viestintäsalaisuuden loukkauksesta ja törkeästä viestintäsalaisuuden loukkauksesta säädetään 38 luvun 3 ja 4 §:ssä sekä rangaistus tietomurrosta ja törkeästä tietomurrosta 38 luvun 8 ja 8 a §:ssä. Rangaistus tämän lain 60 §:ssä säädetyn vaitiolo-velvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla laissa säädetä ankarampaa rangaistusta.

60 §

Vaitiolo-velvollisuus

Henkilötietojen käsittelyyn osallistunut henkilö ei saa oikeudettomasti ilmaista sivulliselle näin tietoonsa saamiaan henkilötietoja.

11 luku

Voimaantulo- ja siirtymäsäännökset

61 §

Voimaantulo

Tämä laki tulee voimaan 6 päivänä toukokuuta 2018.

62 §

Siirtymäsäännökset

Ennen 6 päivänä toukokuuta 2016 luodut automatisoidut käsittelyjärjestelmät on saatettava 19 §:n mukaisiksi viimeistään 6 päivänä toukokuuta 2023.

Tämän lain Tietosuojavirastoa koskevia säännöksiä sovelletaan tietosuojalain (/) tultua voimaan. Siihen saakka tämän lain noudattamista valvoo tietosuojavaltuutettu sen mukaan kuin henkilötietolaissa säädetään.

2.

Laki rikosrekisterilain 1 ja 6 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rikosrekisterilain (770/1993) 1 §:n 1 momentti ja 6 §:n 8 momentti, sellaisina kuin ne ovat, 1 §:n 1 momentti laissa 1093/1999 ja 6 §:n 8 momentti laissa 215/2012, seuraavasti:

1 §

Rikosrekisterin tarkoitus ja tiedot

Rikosrekisterin rekisterinpitäjä on Oikeusrekisterikeskus.

6 §

— — —

Sillä jolla on oikeus kirjoittaa oikeushenkilön nimi, on oikeus pyynnöstä saada tämän lain 5 §:n 1 momentissa tarkoitettu oikeushenkilöä koskeva ote rikosrekisteristä.

3.

Laki

**rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden
Euroopan unionin jäsenvaltioiden välillä annetun lain muuttamisesta**

Eduskunnan päätöksen mukaisesti

muutetaan rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä annetun lain (214/2012) 4 §:n 3 momentti, 8 § ja 13 §, seuraavasti:

4 §

Suhde muihin lakeihin ja kansainvälisiin velvoitteisiin

— — —

Jollei tässä tai muussa laissa toisin säädetä, henkilötietojen salassapitoon, luovuttamiseen ja suojaamiseen sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä muuhun henkilötietojen käsittelyyn henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (/).

8 §

Säilytysrekisterin käyttötarkoitus

Säilytysrekisterin rekisterinpitäjä on Oikeusrekisterikeskus. Säilytysrekisteriä pidetään tietojen säilyttämistä varten niiden edelleen luovuttamiseksi toisiin jäsenvaltioihin ja Suomen viranomaisille sekä rikosrekisteriotteelle merkitsemiseksi siten kuin tässä laissa säädetään.

13 §

Tarkastusoikeus

Henkilön oikeudesta tarkastaa häntä koskevat rekisteritiedot säädetään erikseen.

4.

Laki
oikeushallinnon valtakunnallisesta tietojärjestelmästä annetun lain
muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan oikeushallinnon valtakunnallisesta tietojärjestelmästä annetun lain (372/2010) 18 §:n 2 momentti, ja

muutetaan 2 §:n 1 momentti, 10 §:n 2 momentti ja 19 §, seuraavasti:

2 §

Suhde muuhun lainsäädäntöön

Tässä laissa säädetyn lisäksi tietojen luovuttamisesta oikeushallinnon valtakunnallisesta tietojärjestelmästä ja siihen talletettujen tietojen julkisuudesta säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja henkilötietojen käsittelystä luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa asetuksessa (EU) 2016/679, tietosuojalaissa (/) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (/).

— — —

10 §

Tietojärjestelmään talletettavat henkilötiedot

— — —

Asiaan osallisesta luonnollisesta henkilöstä saa ratkaisu- ja päätösilmoitusjärjestelmään tallettaa vain sellaisia henkilötietojen käsittelystä yleisen tietosuoja-asetuksen 9 artiklassa tarkoitettuja arkaluonteisia tietoja, jotka on talletettava tuomioistuimen diaari- tai muuhun asiakirjarekisteriin tai jotka ilmenevät oikeushallinnon viranomaisen ratkaisusta ja jotka ovat tarpeellisia tuomion täytäntöön panemiseksi, merkinnän tekemiseksi viranomaisen rekisteriin tai muiden oikeushallinnon viranomaisten laissa säädettyjen tehtävien hoitamiseksi.

19 §

Tarkastusoikeuden toteuttaminen ja tietojen korjaaminen

Rekisteröidyn tarkastusoikeudesta ja oikeudesta saada itseään koskevat tiedot oikaisu-
tua tai täydennettyä säädetään erikseen.

5.

Laki

sakon täytäntöönpanosta annetun lain 46 §:n ja 49 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sakon täytäntöönpanosta annetun lain (672/2002) 49 § ja

muutetaan 46 §:n 3 momentti, seuraavasti:

46 §

Sakkorekisterin käyttötarkoitus ja rekisterin tietojen käsittely

— — —

Sen lisäksi mitä tässä tai muussa laissa säädetään, oikeudesta saada tieto viranomaisen julkisista asiakirjoista sekä viranomaisen vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) sekä muusta henkilötietojen käsittelystä luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa asetuksessa (EU) 2016/679, tietosuojalaissa (/) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (/).

6.

Laki henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain (1069/2015) 1, 30, ja 31 §, 33 §:n 1 momentti sekä 37 §:n 2 momentti, seuraavasti:

1 §

Lain soveltamisala

Tässä laissa säädetään rangaistusten täytäntöönpanon sekä muiden Rikosseuraamuslaitokselle kuuluvien tehtävien suorittamiseksi tarpeellisten henkilörekisterien pitämisestä ja muusta henkilötietojen käsittelystä. Jollei tässä laissa toisin säädetä, henkilötietojen salassapitoon ja luovuttamiseen sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä muuhun henkilötietojen käsittelyyn luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettua asetusta (EU) 2016/679 (jäljempänä *yleinen tietosuojasetus*), tietosuojalakia (/) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettu lakia (/).

30 §

Tietojen käsittelystä ilmoittaminen

Rekisterinpitäjän on ilmoitettava rekisteröidylle tietojen käsittelystä sen mukaan kuin yleisessä tietosuojasetuksessa ja tietosuojalaissa säädetään. Tiedonantovelvollisuudesta voidaan kuitenkin poiketa, jos se on välttämätöntä Rikosseuraamuslaitoksen yksikön järjestyksen ja turvallisuuden vuoksi.

31 §

Tarkastusoikeuden rajoitukset

Sen lisäksi, mitä yleisessä tietosuojasetuksessa, tietosuojalaissa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä

annetussa laissa säädetään, rekisteröidyn tarkastusoikeutta voidaan rajoittaa, jos tarkastusoikeuden toteuttamisesta voi todennäköisin syin seurata vakava uhka Rikosseuraamuslaitoksen yksikön järjestykselle ja turvallisuudelle taikka Rikosseuraamuslaitoksen henkilöstöön kuuluvan tai jonkun muun turvallisuudelle. Rekisteröidyllä ei ole tarkastusoikeutta turvallisuustietorekisterin tietoihin eikä valvonta- ja toimintarekisterin sisältämiin tämän lain 7 §:n 1 momentin 10 kohdassa tarkoitettuihin asianomistajan tietoihin.

Tietosuojavirasto voi rekisteröidyn pyynnöstä tarkastaa 1 momentissa tarkoitettujen rekisteröityä koskevien tietojen lainmukaisuuden.

33 §

Virheelliseksi todetun tiedon säilyttäminen

Sen estämättä, mitä yleisessä tietosuojasetuksessa, tietosuojalaissa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa säädetään rekisterissä olevan virheellisen tiedon korjaamisesta, virheelliseksi todettu tieto saadaan säilyttää korjatun tiedon yhteydessä, jos se on tarpeen rekisteröidyn, muun asianosaisen tai Rikosseuraamuslaitoksen henkilöstöön kuuluvan oikeuksien turvaamiseksi. Tällaista tietoa saadaan käyttää vain mainitussa tarkoituksessa.

37 §

Rangaistussäännökset

Rangaistus tietosuojarikoksesta tuomitaan rikoslain 38 luvun 9 §:n mukaan ja henkilörekisteriin kohdistuvasta tietomurrosta rikoslain 38 luvun 8 §:n mukaan.

7.

**Laki
ulosottokaaren 1 luvun 27 ja 28 §:n muuttamisesta**

Eduskunnan päätöksen mukaisesti

muutetaan ulosottokaaren (705/2007) 1 luvun 27 §:n 1 momentti ja 28 §, seuraavasti:

27 §

Oikeus käsitellä tietoja

Ulosottorekisteriä varten kerättyjen ja siihen talletettujen henkilötietojen käsittelystä säädetään tämän lain lisäksi yleisessä tietosuoja-asetuksessa, tietosuoja-laissa (/) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (/).

28 §

Rekisteröidyn tarkastusoikeuden rajoittaminen

Rekisteröidyn tarkastusoikeudesta säädetään yleisessä tietosuoja-asetuksessa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa. Jos rekisteröidyn tarkastusoikeus tuntuvasti vaikeuttaisi täytäntöönpanoa, tarkastusoikeutta voidaan tarpeellisin osin lykätä, kunnes tarvittavat ulosmittaukset tai muut täytäntöönpanotoimet on suoritettu ja omaisuus on otettu ulosottomiehen haltuun, enintään kuitenkin kuusi kuukautta tarkastusoikeutta koskevan pyynnön esittämisestä.

RINNAKKAISTEKSTIT

2.

Laki rikosrekisterilain 1 ja 6 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rikosrekisterilain (770/1993) 1 §:n 1 momentti ja 6 §:n 8 momentti, sellaisina kuin ne ovat, 1 §:n 1 momentti laissa 1093/1999 ja 6 §:n 8 momentti laissa 215/2012, seuraavasti:

Voimassa oleva laki

Ehdotus

1 §

Oikeusrekisterikeskus pitää yllä rikosrekisteriä siten kuin tässä laissa säädetään.

6 §

Henkilön oikeudesta tarkastaa häntä koskevat rekisteritiedot säädetään erikseen. Rikosrekisteriin merkityllä on lisäksi oikeus pyynnöstä saada tieto siitä, kenelle ja mihin tarkoitukseen hänestä on annettu tietoja automaattisen tietojenkäsittelyn avulla pidettävästä rekisteristä viimeisen vuoden aikana. Sillä, jolla on oikeus kirjoittaa oikeushenkilön nimi, on rekisterin pitämismenetelmästä riippumatta vastaava tarkastus- ja tiedonsaantioikeus oikeushenkilön puolesta sekä oikeus saada sitä koskeva ote rekisteristä.

1 §

Rikosrekisterin rekisterinpitäjä on Oikeusrekisterikeskus.

6 §

Sillä jolla on oikeus kirjoittaa oikeushenkilön nimi, on oikeus pyynnöstä saada tämän lain 5 §:n 1 momentissa tarkoitettu oikeushenkilöä koskeva ote rikosrekisteristä.

3.

Laki

rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rikosrekisteritietojen säilyttämisestä ja luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä annetun lain (214/2012) 4 §:n 3 momentti, 8 § ja 13 §, seuraavasti:

Voimassa oleva laki

4 §

Suhde muihin lakeihin ja kansainvälisiin velvoitteisiin

— — —

Jollei tässä tai muussa laissa toisin säädetä, henkilötietojen salassapitoon, luovuttamiseen ja suojaamiseen sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä muuhun henkilötietojen käsittelyyn henkilötietolakia (523/1999).

8 §

Säilytysrekisterin käyttötarkoitus

Oikeusrekisterikeskus pitää yllä säilytysrekisteriä. Säilytysrekisteriä pidetään tietojen säilyttämistä varten niiden edelleen luovuttamiseksi toisiin jäsenvaltioihin ja Suomen viranomaisille sekä rikosrekisteriotteelle merkitsemiseksi siten kuin tässä laissa säädetään.

13 §

Tarkastusoikeus

Henkilön oikeudesta tarkastaa häntä koskevat rekisteritiedot säädetään erikseen. *Säilytysrekisteriin merkityllä on lisäksi oikeus pyynnöstä saada tieto siitä, kenelle ja mihin tarkoitukseen hänestä on annettu tietoja automaattisen tietojenkäsittelyn avulla pidettävästä rekisteristä viimeisen vuoden aikana.*

Ehdotus

4 §

Suhde muihin lakeihin ja kansainvälisiin velvoitteisiin

— — —

Jollei tässä tai muussa laissa toisin säädetä, henkilötietojen salassapitoon, luovuttamiseen ja suojaamiseen sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia ([621/1999](#)) sekä muuhun *henkilötietojen käsittelyyn henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (/).*

8 §

Säilytysrekisterin käyttötarkoitus

Säilytysrekisterin rekisterinpitäjä on Oikeusrekisterikeskus. Säilytysrekisteriä pidetään tietojen säilyttämistä varten niiden edelleen luovuttamiseksi toisiin jäsenvaltioihin ja Suomen viranomaisille sekä rikosrekisteriotteelle merkitsemiseksi siten kuin tässä laissa säädetään.

13 §

Tarkastusoikeus

Henkilön oikeudesta tarkastaa häntä koskevat rekisteritiedot säädetään erikseen.

4.

Laki

oikeushallinnon valtakunnallisesta tietojärjestelmästä annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan oikeushallinnon valtakunnallisesta tietojärjestelmästä annetun lain (372/2010) 18 §:n 2 momentti, ja

muutetaan 2 §:n 1 momentti, 10 §:n 2 momentti ja 19 §, seuraavasti:

Voimassa oleva laki

2 §

Suhde muuhun lainsäädäntöön

Jollei tässä laissa toisin säädetä, tietojen luovuttamisesta oikeushallinnon valtakunnallisesta tietojärjestelmästä ja siihen talletettujen tietojen julkisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, ja muusta tietojärjestelmään talletettujen henkilötietojen käsittelystä, mitä henkilötietolaissa (523/1999) säädetään.

10 §

Tietojärjestelmään talletettavat henkilötiedot

Asiaan osallisesta luonnollisesta henkilöstä saa ratkaisu- ja päätösilmoitusjärjestelmään tallettaa vain sellaisia henkilötietolain 11 §:ssä tarkoitettuja arkaluonteisia tietoja, jotka on talletettava tuomioistuimen diaari- tai muuhun asiakirjarekisteriin tai jotka ilmenevät oikeushallinnon viranomaisen ratkaisusta ja jotka ovat tarpeellisia tuomion täytäntöön panemiseksi, merkinnän tekemiseksi viranomaisen rekisteriin tai muiden oikeushallinnon viranomaisten laissa säädettyjen tehtävien hoitamiseksi.

2 §

Suhde muuhun lainsäädäntöön

Tässä laissa säädetyn lisäksi tietojen luovuttamisesta oikeushallinnon valtakunnallisesta tietojärjestelmästä ja siihen talletettujen tietojen julkisuudesta säädetään viranomaisten toiminnan julkisuudesta annetussa laissa ([621/1999](#)) ja *henkilötietojen käsittelystä luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta* annetussa asetuksessa (EU) 2016/679, *tietosuojalaissa* (/) sekä *henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä* annetussa laissa (/).

10 §

Tietojärjestelmään talletettavat henkilötiedot

Asiaan osallisesta luonnollisesta henkilöstä saa ratkaisu- ja päätösilmoitusjärjestelmään tallettaa vain sellaisia henkilötietojen käsittelystä *yleisen tietosuojasetuksen 9 artiklassa* tarkoitettuja arkaluonteisia tietoja, jotka on talletettava tuomioistuimen diaari- tai muuhun asiakirjarekisteriin tai jotka ilmenevät oikeushallinnon viranomaisen ratkaisusta ja jotka ovat tarpeellisia tuomion täytäntöön panemiseksi, merkinnän tekemiseksi viranomaisen rekisteriin tai muiden oikeushallinnon viranomaisten laissa säädettyjen tehtävien hoitamiseksi.

18 §

Tietojen poistaminen

Raportointi-, tilasto- ja arkistojärjestelmään talletettujen tietojen poistamiseen sovelletaan, mitä henkilötietolaissa säädetään tai sen nojalla päätetään.

19 §

Tarkastusoikeuden toteuttaminen ja tietojen korjaaminen

Oikeushallinnon viranomainen käsittelee ja ratkaisee rekisteröidyn tarkastusoikeutta ja tietojen korjaamista koskevan pyynnön, joka koskee yksinomaan asianomaisen viranomaisen käsittelemää ja ratkaistavaa asiaa ja jota koskevat tiedot asianomainen viranomainen on tallettanut oikeushallinnon valtakunnalliseen tietojärjestelmään.

Oikeusrekisterikeskus voi siirtää rekisteröidyn sille esittämän pyynnön tarkastusoikeutensa toteuttamisesta tai itseään koskevien henkilötietojen oikaisemisesta sille oikeushallinnon viranomaiselle, joka on tallettanut rekisteröityä koskevat tiedot ratkaisuja päätösilmoitusjärjestelmään taikka diaari- ja asianhallintatietojen valtakunnalliseen käsittelyjärjestelmään.

Sen estämättä, mitä henkilötietolain 27 §:ssä säädetään tilastointi- tai tutkimustarkoituksia varten pidettyn rekisterin tietojen tarkastusoikeudesta, rekisteröidyllä on tarkastusoikeus, jos Oikeusrekisterikes-

kus on tämän lain 13 §:n nojalla käyttänyt raportointi-, tilasto- ja arkistojärjestelmään siirrettyjä tietoja häntä koskevan asian käsittelyssä.

Rekisteröidyn tarkastusoikeuden toteuttamiseen sovelletaan muutoin, mitä henkilötietolaissa säädetään.

(kumotaan)

19 §

Tarkastusoikeuden toteuttaminen ja tietojen korjaaminen

Rekisteröidyn tarkastusoikeudesta ja oikeudesta saada itseään koskevat tiedot oikaistua tai täydennettyä säädetään erikseen.

5.

Laki sakon täytäntöönpanosta annetun lain 46 §:n ja 49 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sakon täytäntöönpanosta annetun lain (672/2002) 49 § ja

muutetaan 46 §:n 3 momentti, seuraavasti:

46 §

*Sakkorekisterin käyttötarkoitus ja rekisterin
tietojen käsittely*

Sakkorekisterin tietojen käsittelyyn sovelletaan henkilötietolakia (523/1999) ja tietojen luovuttamisen osalta viranomaisten toiminnan julkisuudesta annettua lakia (621/1999), jollei jäljempänä toisin säädetä.

49 §

Vastuu sakkorekisteriin talletetuista tiedoista

Oikeusrekisterikeskus vastaa sakkorekisteriin talletettujen tietojen virheettömyydestä ja rekisterin käytön laillisuudesta. Rekisterinpitäjä on velvollinen korvaamaan taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle virheellisiin tietoihin liittyvästä tai muusta lainvastaisesta sakkorekisteriin talletettujen tietojen käsittelystä. Vahingonkorvauslakia (412/1974) sovelletaan siten kuin henkilötietolain 47 §:n 2 momentissa säädetään.

46 §

*Sakkorekisterin käyttötarkoitus ja rekisterin
tietojen käsittely*

Sen lisäksi mitä tässä tai muussa laissa säädetään, oikeudesta saada tieto viranomaisen julkisista asiakirjoista sekä viranomaisen vaitiovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista säädetään viranomaisten toiminnan julkisuudesta annetussa laissa ([621/1999](#)) sekä muusta henkilötietojen käsittelystä luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa asetuksessa (EU) 2016/679, tietosuojalaissa (/) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (/).

(49 § kumotaan)

Laki

henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain (1069/2015) 1, 30, ja 31 §, 33 §:n 1 momentti sekä 37 §:n 2 momentti, seuraavasti:

Voimassa oleva lainsäädäntö

Ehdotus

1 §

1 §

Lain soveltamisala

Lain soveltamisala

Tässä laissa säädetään rangaistusten täytäntöönpanon sekä muiden Rikosseuraamuslaitokselle kuuluvien tehtävien suorittamiseksi tarpeellisten henkilörekisterien pitämisestä ja muusta henkilötietojen käsittelystä. Jollei tässä laissa toisin säädetä, henkilötietojen salassapitoon ja luovuttamiseen sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä muuhun henkilötietojen käsittelyyn henkilötietolakia (523/1999).

Tässä laissa säädetään rangaistusten täytäntöönpanon sekä muiden Rikosseuraamuslaitokselle kuuluvien tehtävien suorittamiseksi tarpeellisten henkilörekisterien pitämisestä ja muusta henkilötietojen käsittelystä. Jollei tässä laissa toisin säädetä, henkilötietojen salassapitoon ja luovuttamiseen sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä muuhun henkilötietojen käsittelyyn *luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettua asetusta (EU) 2016/679 (jäljempänä yleinen tietosuoja-asetus), tietosuojalakia (/)* sekä *henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettu lakia (/)*.

30 §

30 §

Tietojen käsittelystä ilmoittaminen

Tietojen käsittelystä ilmoittaminen

Rekisterinpitäjän on ilmoitettava rekisteröidylle tietojen käsittelystä siten kuin henkilötietolaissa säädetään. Tiedonantovelvollisuudesta voidaan kuitenkin poiketa, jos se on välttämätöntä Rikosseuraamuslaitoksen yksikön järjestyksen ja turvallisuuden vuoksi.

Rekisterinpitäjän on ilmoitettava rekisteröidylle tietojen käsittelystä *sen mukaan kuin yleisessä tietosuoja-asetuksessa ja tietosuojalaissa säädetään*. Tiedonantovelvollisuudesta voidaan kuitenkin poiketa, jos se on välttämätöntä Rikosseuraamuslaitoksen yksikön järjestyksen ja turvallisuuden vuoksi.

Tarkastusoikeuden rajoitukset

Sen lisäksi, mitä henkilötietolaissa säädetään, rekisteröidyn tarkastusoikeutta voidaan rajoittaa, jos tarkastusoikeuden toteuttamisesta voi todennäköisin syin seurata vakava uhka Rikosseuraamuslaitoksen yksikön järjestykselle ja turvallisuudelle taikka Rikosseuraamuslaitoksen henkilöstöön kuuluvan tai jonkun muun turvallisuudelle. Rekisteröidyllä ei ole tarkastusoikeutta turvallisuustietorekisterin tietoihin eikä valvonta- ja toimintarekisterin sisältämiin tämän lain 7 §:n 1 momentin 10 kohdassa tarkoitettuihin asianomistajan tietoihin. (8.1.2016/17)

Tietosuoja-valtuutettu voi rekisteröidyn pyynnöstä tarkastaa 1 momentissa tarkoitettujen rekisteröityä koskevien tietojen lainmukaisuuden.

Virheelliseksi todetun tiedon säilyttäminen

Sen estämättä, mitä henkilötietolaissa säädetään rekisterissä olevan virheellisen tiedon korjaamisesta, virheelliseksi todettu tieto saadaan säilyttää korjatun tiedon yhteydessä, jos se on tarpeen rekisteröidyn, muun asianosaisen tai Rikosseuraamuslaitoksen henkilöstöön kuuluvan oikeuksien turvaamiseksi. Tällaista tietoa saadaan käyttää vain mainitussa tarkoituksessa.

Tarkastusoikeuden rajoitukset

Sen lisäksi, mitä yleisessä tietosuoja-asetuksessa, tietosuoja-laissa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa säädetään, rekisteröidyn tarkastusoikeutta voidaan rajoittaa, jos tarkastusoikeuden toteuttamisesta voi todennäköisin syin seurata vakava uhka Rikosseuraamuslaitoksen yksikön järjestykselle ja turvallisuudelle taikka Rikosseuraamuslaitoksen henkilöstöön kuuluvan tai jonkun muun turvallisuudelle. Rekisteröidyllä ei ole tarkastusoikeutta turvallisuustietorekisterin tietoihin eikä valvonta- ja toimintarekisterin sisältämiin tämän lain 7 §:n 1 momentin 10 kohdassa tarkoitettuihin asianomistajan tietoihin.

Tietosuoja-virasto voi rekisteröidyn pyynnöstä tarkastaa 1 momentissa tarkoitettujen rekisteröityä koskevien tietojen lainmukaisuuden.

Virheelliseksi todetun tiedon säilyttäminen

Sen estämättä, mitä yleisessä tietosuoja-asetuksessa, tietosuoja-laissa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa säädetään rekisterissä olevan virheellisen tiedon korjaamisesta, virheelliseksi todettu tieto saadaan säilyttää korjatun tiedon yhteydessä, jos se on tarpeen rekisteröidyn, muun asianosaisen tai Rikosseuraamuslaitoksen henkilöstöön kuuluvan oikeuksien turvaamiseksi. Tällaista tietoa saadaan käyttää vain mainitussa tarkoituksessa.

37 §

Rangaistussäännökset

Rangaistus henkilörekisteririkoksesta tuomitaan [rikoslain 38 luvun 9 §:n](#) mukaan ja henkilörekisteriin kohdistuvasta tietomurrosta [rikoslain 38 luvun 8 §:n](#) mukaan. *Rangaistus henkilörekisteririkkomuksesta tuomitaan henkilötietolain 48 §:n 2 momentin mukaan.*

37 §

Rangaistussäännökset

Rangaistus *tietosuoja*rikoksesta tuomitaan rikoslain 38 luvun 9 §:n mukaan ja henkilörekisteriin kohdistuvasta tietomurrosta rikoslain 38 luvun 8 §:n mukaan.

Laki
ulosottokaaren 1 luvun 27 ja 28 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan ulosottokaaren (705/2007) 1 luvun 27 §:n 1 momentti ja 28 §, seuraavasti

27 §

Oikeus käsitellä tietoja

Ulosottorekisteriä varten kerättyjen ja siihen talletettujen henkilötietojen käsittelyyn sovelletaan henkilötietolakia, jollei jäljempänä toisin säädetä.

27 §

Oikeus käsitellä tietoja

Ulosottorekisteriä varten kerättyjen ja siihen talletettujen henkilötietojen *käsittelystä säädetään tämän lain lisäksi yleisessä tietosuoja-asetuksessa, tietosuojalaissa (/) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (/)*.

— — —

28 §

Rekisteröidyn tarkastusoikeus

Jos henkilötietolain mukainen rekisteröidyn tarkastusoikeus tuntuvasti vaikeuttaisi täytäntöönpanoa, tarkastusoikeutta voidaan tarpeellisin osin lykätä, kunnes tarvittavat ulosmittaukset tai muut täytäntöönpanotoimet on suoritettu ja omaisuus on otettu ulosottomiehen haltuun, enintään kuitenkin kuusi kuukautta tarkastusoikeutta koskevan pyynnön esittämisestä.

Jos tarkastusoikeutta on lykätty, tietosuojavaltuutettu voi sen lisäksi, mitä muualla säädetään, rekisteröidyn pyynnöstä tarkastaa rekisterissä olevien rekisteröityä koskevien tietojen lainmukaisuuden

28 §

Rekisteröidyn tarkastusoikeuden rajoittaminen

Rekisteröidyn tarkastusoikeudesta säädetään yleisessä tietosuoja-asetuksessa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa. Jos rekisteröidyn tarkastusoikeus tuntuvasti vaikeuttaisi täytäntöönpanoa, tarkastusoikeutta voidaan tarpeellisin osin lykätä, kunnes tarvittavat ulosmittaukset tai muut täytäntöönpanotoimet on suoritettu ja omaisuus on otettu ulosottomiehen haltuun, enintään kuitenkin kuusi kuukautta tarkastusoikeutta koskevan pyynnön esittämisestä.

LAGFÖRSLAG

1.

Lag

om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

Denna lag tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter när det är fråga om att

1. förebygga, förhindra, avslöja och utreda brott och föra brott till åtalsprövning,
2. åtalspröva och bedriva annan åklagarverksamhet som hänför sig till brott,
3. behandla brottmål i domstol,
4. verkställa straffrättsliga påföljder, eller
5. skydda mot samt förebygga eller förhindra hot mot den allmänna säkerheten i samband med verksamhet som avses i 1–4 punkten.

Utöver vad som föreskrivs i 1 mom. tillämpas denna lag på

1. sådan behandling av personuppgifter som utförs av försvarsmakten och för försvarsmaktens räkning, när uppgifterna behandlas för skötsel av uppgifter som anges i 2 § 1 mom. i lagen om försvarsmakten (551/2007),
2. sådan behandling av personuppgifter som utförs av polisen, när uppgifterna behandlas inom ramen för en i 1 § 1 mom. i polislagen (872/2011) avsedd uppgift som hänför sig till skyddandet av den nationella säkerheten, och
3. sådan behandling av personuppgifter som utförs av gränsbevakningsväsendet, när uppgifterna behandlas inom ramen för en i 3 § 2 och 3 mom. i gränsbevakningslagen (578/2005) avsedd uppgift som hänför sig till skyddandet av den nationella säkerheten.

På sådan behandling av personuppgifter som avses i 2 mom. tillämpas dock inte 7 kap. i denna lag.

Denna lag tillämpas dock endast på sådan behandling av personuppgifter enligt 1 och 2 mom. som är helt eller delvis automatiserad eller där de uppgifter som behandlas utgör eller är avsedda att utgöra ett register eller en del av ett sådant.

Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (*dataskyddsdirektivet*).

2 §

Förhållande till annan lagstiftning

Om det i någon annan lag finns bestämmelser som avviker från denna lag, ska de tillämpas i stället för denna lag.

Bestämmelser om rätten att ta del av myndigheternas offentliga handlingar samt om tystnadsplikt för den som är verksam vid en myndighet, om handlingssekretess samt andra för skyddande av allmänna och enskilda intressen nödvändiga begränsningar av rätten att ta del av en handling finns i lagen om offentlighet i myndigheternas verksamhet (621/1999).

3 §

Definitioner

I denna lag avses med

1. *personuppgifter* varje upplysning som direkt eller indirekt avser en identifierad eller identifierbar fysisk person (*en registrerad*),
2. *behandling* insamling, registrering, organisering, strukturering, bevaring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller *förstöring* samt någon annan åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller datamängder som innehåller personuppgifter,

3. *begränsning av behandling* markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,
4. *register* en strukturerad datamängd med personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om datamängden är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska *förhållanden*,
5. *behörig myndighet* en offentlig myndighet som har behörighet att förebygga, förhindra, avslöja eller utreda brott eller föra brott till åtalsprövning, åtalspröva och bedriva annan verksamhet som hänför sig till åtal för brott, döma till straffrättsliga påföljder eller verkställa straffrättsliga påföljder, inklusive *skydda* mot eller förhindra hot mot den allmänna säkerheten liksom försvarsmakten, polisen och gränsbevakningsväsendet när de sköter uppgifter som avses i 1 § 2 mom.,
6. *registeransvarig* en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter eller som enligt lag har ålagts skyldighet att föra register,
7. *registerförare* en fysisk eller juridisk person, en *myndighet*, ett ämbetsverk eller något annat organ som behandlar personuppgifter för den registeransvariges räkning,
8. *mottagare* en fysisk eller juridisk person, en myndighet, ett ämbetsverk eller något annat organ till vilket personuppgifterna utlämnas, med undantag av en behörig myndighet som kan komma att få personuppgifter för *ändamål* som anges i 1 § 1 mom. i denna lag inom ramen för ett särskilt uppdrag,
9. *personuppgiftsincident* brott mot bestämmelserna om informationssäkerhet vilket leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de *personuppgifter* som överförts, lagrats eller på annat sätt behandlats,
10. *lämpliga skyddsåtgärder* sådana tekniska och organisatoriska åtgärder som säkerställer att behandlingen av personuppgifter är laglig, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerades rättigheter,
11. *genetiska uppgifter* alla personuppgifter som rör sådana nedärvda eller förvärvade genetiska kännetecken för en fysisk person som ger unik information om denna fysiska persons fysiologi eller hälsa och vilka härrör från en analys av ett biologiskt prov från den fysiska personen i fråga eller på annat sätt,
12. *biometrisk uppgift* personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, *fysiologiska* eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av denna fysiska person,
13. *uppgifter om hälsa* personuppgifter som rör en persons fysiska eller psykiska hälsa och som ger information om dennes hälsotillstånd,
14. *tredjeland* ett land som inte är *medlemsstat* i Europeiska unionen (EU), ett annat land inom Europeiska ekonomiska samarbetsområdet eller Schweiz,

15. *internationell organisation* en organisation och dess underställda organ som lyder under folkrätten samt ett annat organ som har inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

Vad som i denna lag föreskrivs om behörig myndighet tillämpas också på enskilda som sköter en uppgift som avses i 1 mom. 5 punkten.

Vad som i denna lag föreskrivs om en medlemsstat i Europeiska unionen tillämpas också på andra länder inom Europeiska ekonomiska samarbetsområdet och på Schweiz.

2 kap.

Allmänna förutsättningar för behandling av personuppgifter

4 §

Laglighetskrav

Personuppgifter får behandlas endast om det föreskrivs om behandlingen i lag och behandlingen behövs för att en behörig myndighet ska kunna utföra en uppgift enligt 1 §.

Personuppgifter ska behandlas på ett korrekt och omsorgsfullt sätt.

5 §

Ändamålsbundenhet

Personuppgifter får samlas in endast för särskilda, uttryckligt angivna ändamål. De får inte behandlas på ett sätt som är oförenligt med dessa ändamål.

Personuppgifter som har samlats in för ett ändamål som anges i 1 § får behandlas för något annat än ett i 1 § angivet ändamål endast om det föreskrivs om behandlingen i lag.

Samma eller en annan registeransvarig får behandla personuppgifter också för arkivändamål av allmänt intresse och för vetenskaplig, statistisk eller historisk användning, under förutsättning att lämpliga skyddsåtgärder för de registrerades rättigheter har vidtagits.

6 §

Relevanskrav

De personuppgifter som behandlas ska vara adekvata och behövliga med tanke på ändamålet med behandlingen och får inte vara för omfattande i förhållande till de ändamål för vilka de behandlas. Obehövliga personuppgifter ska raderas utan obefogat dröjsmål.

Personuppgifter får inte bevaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som behövs med tanke på ändamålet med behandlingen.

Behovet av bevaring av personuppgifter ska bedömas med minst fem års mellanrum, om inte något annat föreskrivs om bevaringstider för personuppgifter någon annanstans.

7 §

Felfrihetskrav

De personuppgifter som behandlas ska vara felfria och uppdaterade med hänsyn till ändamålet med behandlingen.

8 §

Åtskillnad mellan olika personuppgifter

Den registeransvarige ska vid behov och så långt det är möjligt göra en klar åtskillnad mellan personuppgifter som avser registrerade i olika ställning med tanke på det ärende som behandlas.

Alla rimliga åtgärder ska vidtas för att personuppgifter som grundar sig på fakta åtskiljs från personuppgifter som grundar sig på personliga bedömningar.

9 §

Säkerställande av kvaliteten på personuppgifter som överförs eller görs tillgängliga

Den behöriga myndigheten ska vidta alla rimliga åtgärder för att se till att personuppgifter som är oriktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga.

Vid all överföring av personuppgifter ska, så långt det är möjligt, sådan information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga, tillförlitliga och aktuella.

Om det visar sig att oriktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts, ska mottagaren omedelbart informeras om detta. Efter att mottagaren informerats om saken ska denne rätta eller radera personuppgifterna eller begränsa behandlingen av dem.

10 §

Skyldighet att informera om särskilda förutsättningar för behandlingen

Om det i lag anges särskilda förutsättningar för behandling av personuppgifter, ska den behöriga myndigheten i samband med överlåtelse eller överföring av personuppgifter informera mottagaren av personuppgifterna om dessa förutsättningar samt om skyldigheten att iaktta dem.

När den behöriga myndigheten överför personuppgifter till en mottagare inom Europeiska unionen får den inte uppställa strängare krav på behandlingen av personuppgifter än vad som tillämpas nationellt på likartade uppgiftsöverföringar.

11 §

Behandling av särskilda kategorier av personuppgifter

Uppgifter som hör till särskilda kategorier av personuppgifter (*känsliga personuppgifter*) är personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt genetiska uppgifter, biometrisk uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Känsliga personuppgifter får behandlas endast om det är nödvändigt och under förutsättning att skyddsåtgärder som krävs för att trygga den registrerades rättigheter har vidtagits och om

1. det föreskrivs om behandlingen i lag,
2. det är nödvändigt för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller
3. behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

12 §

Behandling av personbeteckning

En personbeteckning får behandlas endast om en entydig individualisering av den registrerade är viktig

1. för att en behörig myndighet ska kunna utföra en uppgift som ålagts den i lag,
2. för att tillgodose den registrerades eller den registeransvariges rättigheter eller skyldigheter, eller
3. för sådan historisk eller vetenskaplig forskning eller statistikföring som anges i 5 § 3 mom.

En personbeteckning får inte onödigt antecknas i handlingar som skrivs ut eller upprättas på basis av ett personregister.

13 §

Automatiserat individuellt beslutsfattande

Det är förbjudet att fatta beslut som enbart grundas på automatiserad behandling av personuppgifter och som har negativa rättsverkningar för den registrerade eller annars är betydande för denne, om inte något annat föreskrivs i lag.

3 kap.

Registeransvarig och registerförare

14 §

Den registeransvariges ansvar

Den registeransvarige svarar för att personuppgifter behandlas i enlighet med lag.

Den registeransvarige ska vidta behövliga tekniska och organisatoriska åtgärder för att kunna säkerställa och visa att behandlingen av personuppgifter utförs i enlighet med lag. I samband med åtgärderna ska behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter beaktas.

15 §

Inbyggt dataskydd och dataskydd som standard

Den registeransvarige ska vid beslut om hur behandlingen av personuppgifter ska utföras och vid själva behandlingen av personuppgifter genomföra lämpliga tekniska och organisatoriska skyddsåtgärder för att säkerställa att behandlingen utförs i enlighet med lag och den registrerades rättigheter skyddas. Åtgärderna ska vidtas med beaktande av tillgängliga tekniska lösningar, genomförandekostnaderna samt behandlingens art, omfattning, sammanhang och ändamål samt de risker som behandlingen innebär för personens rättigheter.

Den registeransvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att i standardfallet säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.

16 §

Gemensamt registeransvariga

Om två eller flera registeransvariga gemensamt fastställer behandlingens ändamål och medel, ska de komma överens om den inbördes ansvarsfördelningen vid skötseln av skyldigheter enligt denna lag, om det inte föreskrivs om ansvarsfördelningen i lag.

De registeransvariga som avses i 1 mom. ska inom sig utse en registeransvarig som fungerar som kontaktpunkt och med vilken den registrerade kan ha kontakt i ärenden

som gäller utövandet av den registrerades rättigheter. Den registrerade får dock alltid utöva sina rättigheter enligt denna lag i förhållande till var och en av de registeransvariga.

17 §

Registerförare

Den som behandlar personuppgifter för den registeransvariges räkning ska ge den registeransvarige lämpliga utredningar och förbindelser och även i övrigt tillräckliga garantier för de organisatoriska och tekniska åtgärder genom vilka den säkerställer att personuppgifterna behandlas i enlighet med kraven i denna lag.

Registerföraren får inte behandla personuppgifter på ett sätt som avviker från den registeransvariges instruktioner och inte överföra behandlingen av personuppgifter på någon annan utan skriftligt tillstånd av den registeransvarige.

Ett skriftligt avtal eller ett skriftligt förordnande ska upprättas över den behandling som registerföraren utför, i vilket typen av personuppgifter, behandlingens varaktighet, art och ändamål, kategorierna av personuppgifter och kategorierna av registrerade samt den registeransvariges skyldigheter och rättigheter anges. I ovannämnda skriftliga dokument ska det dessutom anges att registerföraren

1. endast handlar enligt instruktioner från den personuppgiftsansvarige,
2. säkerställer att de fysiska personer som behandlar personuppgifterna har förbundit sig att iaktta sekretess eller att de omfattas av en lagstadgad tystnadsplikt,
3. på lämpligt sätt bistår den registeransvarige för att säkerställa efterlevnad av bestämmelserna om den registrerades rättigheter,
4. beroende på den registeransvariges val, raderar eller återlämnar alla personuppgifter till den registeransvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats och raderar befintliga kopior, om det inte föreskrivs om bevaring av personuppgifterna i lag,
5. ger den registeransvarige tillgång till all information som behövs för att visa att denna paragraf efterlevs,
6. uppfyller de förutsättningar som avses i denna paragraf för anlitan av en annan registerförare.

18 §

Register över behandling

Den registeransvarige ska föra ett skriftligt register över behandling av personuppgifter som denne ansvarar för. Registret ska innehålla följande uppgifter:

1. namn och kontaktuppgifter för den registeransvarige samt vid behov för gemensamt registeransvariga samt för den dataskyddsansvarige som avses i 38 §,
2. ändamålen med och den rättsliga grunden för behandlingen av personuppgifter,
3. en beskrivning av kategorin eller kategorierna av registrerade och av kategorierna av personuppgifter,
4. de kategorier av mottagare som personuppgifterna har lämnats ut till eller ska lämnas ut till,
5. kategorier av personuppgiftsöverföringar till ett tredjeland eller en internationell organisation,
6. om möjligt, de planerade tidsfristerna för radering av de olika kategorierna av personuppgifter,
7. eventuell användning av profilering,
8. om möjligt, en allmän beskrivning av informationssystemen och principerna för skydd av dem samt en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i 31 §.

Registerföraren ska föra ett skriftligt register över all behandling av personuppgifter som utförs för den registeransvariges räkning. Registret ska innehålla följande uppgifter:

1. namn och kontaktuppgifter för registerföraren eller registerförarna samt för den dataskyddsansvarige,
2. namn och kontaktuppgifter för varje registeransvarig för vars räkning registerföraren agerar,
3. de kategorier av behandling som har utförts för varje registeransvarigs räkning,
4. eventuella uppgifter om överföringar av personuppgifter till ett tredjeland eller en internationell organisation, om den registeransvarige uttryckligen gett sådana instruktioner,
5. om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i 31 §.

19 §

Logguppgifter

Den registeransvarige och registerföraren ska bevara logguppgifter över insamling, ändring, läsning, utlämning, överföring, sammanförande och radering av personuppgifter som utförts i deras automatiserade behandlingssystem. Logguppgifterna över läsning och utlämning ska göra det möjligt att utreda grund, datum och tidpunkt för läsning och utlämning och om möjligt vem som har läst eller lämnat ut personuppgifter samt vilka som har fått tillgång till personuppgifterna.

Logguppgifterna får användas endast för att kontrollera om behandlingen utförs i enlighet med lag, för intern kontroll, för att säkerställa personuppgifternas integritet och säkerhet samt inom ramen för straffrättsliga förfaranden.

20 §

Konsekvensbedömning avseende dataskydd

Den registeransvarige ska innan behandlingen av personuppgifter inleds göra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

Om den planerade behandlingen av personuppgifter kan medföra en betydande risk för tillgodoseendet av fysiska personers rättigheter, ska den registeransvarige göra en skriftlig konsekvensbedömning. Konsekvensbedömningen ska innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för den registrerades rättigheter och åtgärder för att minska dem samt åtgärder för att säkerställa skyddet av personuppgifter.

21 §

Förhandssamråd med tillsynsmyndigheten

Den registeransvarige eller registerföraren ska höra Dataskyddsmyndigheten innan personuppgifterna behandlas, om

1. den skriftliga konsekvensbedömning som avses i 20 § 2 mom. visar att behandlingen trots planerade skyddsåtgärder skulle leda till en betydande risk för de registrerades rättigheter, eller

2. behandlingen av uppgifter annars i synnerhet vid användning av ny teknik eller nya rutiner eller förfaranden medför en betydande risk för de registrerades rättigheter.

Dataskyddsmyndigheten får upprätta en förteckning över de behandlingsåtgärder enligt 1 mom. som förutsätter förhandssamråd.

Den registeransvarige ska till Dataskyddsmyndigheten lämna in en skriftlig konsekvensbedömning och på begäran andra sådana uppgifter med vilka myndigheten kan bedöma lagenligheten i behandlingen av personuppgifter.

Om Dataskyddsmyndigheten anser att den behandling som avses i 1 mom. skulle stå i strid med denna lag, ska myndigheten inom sex veckor från det att begäran om samråd mottogs ge den registeransvarige och registerföraren, om en sådan finns, instruktioner i syfte att göra behandlingen lagenlig. Denna period får förlängas med en månad om den planerade behandlingen är så komplicerad att en förlängning krävs. Dataskyddsmyndigheten ska informera den registeransvarige och registerföraren, om en sådan finns, om den förlängda perioden inom en månad från det att begäran om samråd mottogs, tillsammans med orsakerna till förseningen.

4 kap.

De registrerades rättigheter

22 §

Dataskyddsregister som ska göras allmänt tillgängligt

Den registeransvarige ska föra ett skriftligt register över sådan behandling av personuppgifter som denne ansvarar för. Registret ska offentliggöras och innehålla åtminstone följande uppgifter:

1. kontaktuppgifter för den registeransvarige och den dataskyddsansvarige samt, om det anses behövt, den dataskyddsansvariges namn,
2. namn och kontaktuppgifter för den registeransvarige som fungerar som kontaktpunkt för gemensamt registeransvariga samt uppgift om att den registrerade kan utöva sina rättigheter enligt denna lag i förhållande till var och en av de registeransvariga,
3. ändamålen med och den rättsliga grunden för behandlingen av personuppgifter,
4. den period under vilken personuppgifterna kommer att bevaras, eller om den inte har fastställts, de kriterier som används för att fastställa denna period,

5. eventuella regelmässiga mottagare eller kategorier av mottagare av personuppgifterna,
6. uppgift om att den registrerade har rätt att av den registeransvarige begära tillgång till personuppgifter som rör den registrerade samt rätt att begära rättelse eller radering av dessa personuppgifter eller begränsning av behandlingen av dem,
7. uppgift om att den registrerade har rätt att lämna in klagomål enligt 55 § till Dataskyddsmyndigheten samt myndighetens kontaktuppgifter, och
8. eventuella andra uppgifter som behövs för att den registrerade ska kunna utöva sina rättigheter.

23 §

De registrerades rätt till insyn

Var och en har rätt att av den registeransvarige få veta huruvida personuppgifter som gäller honom eller henne håller på att behandlas. Om dessa uppgifter behandlas, har den registrerade rätt att få följande information av den registeransvarige:

1. vilka personuppgifter som håller på att behandlas och all tillgänglig information om varifrån dessa uppgifter härstammar,
2. ändamålen med och den rättsliga grunden för behandlingen,
3. de kategorier av personuppgifter som behandlingen gäller,
4. de mottagare eller kategorier av mottagare till vilka den registrerades personuppgifter ha lämnats ut,
5. den period under vilken personuppgifterna kommer att bevaras, eller om den inte har fastställts, de kriterier som används för att fastställa denna period,
6. rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifter som rör den registrerade eller begränsning av behandling av dem,
7. rätten att lämna in klagomål enligt 55 § till Dataskyddsmyndigheten samt myndighetens kontaktuppgifter.

Den som önskar kontrollera uppgifter om sig själv på det sätt som avses i 1 mom., kan begära detta i en egenhändigt undertecknad eller på ett därmed jämförbart sätt bestyrkt handling eller begära detta personligen hos den registeransvarige.

24 §

Inskränkningar i rätten till insyn

Den registrerades rätt till insyn kan skjutas upp, begränsas eller vägras på de grunder som anges i 28 §. Om den registrerades rätt till insyn skjuts upp, begränsas eller väg-

ras, ska den registeransvarige utan obefogat dröjsmål skriftligen informera den registrerade om detta. Även skälen till uppskov, begränsning eller vägran ska uppges, utom om lämnande av uppgift om dem skulle undergräva ändamålet med vägran eller begränsningen. Om den registeransvarige inte inom tre månader efter att begäran framställts har gett den registrerade ett skriftligt svar, jämställs detta med att insyn har vägrats.

Den registeransvarige ska informera den registrerade om dennes rätt att lämna in ett klagomål till Dataskyddsmyndigheten och att utnyttja rättsmedel på grund av att rätten till insyn skjutits upp, begränsats eller vägrats, liksom om eventuell rätt att utöva rätten till insyn i enlighet med 29 § via Dataskyddsmyndigheten.

Den registeransvarige ska dokumentera information om de skäl som ligger till grund för att rätten till insyn vägrats eller begränsats.

25 §

Rättelse eller radering av personuppgifter eller begränsning av behandling

Den registeransvarige ska på eget initiativ eller på yrkande av den registrerade utan obefogat dröjsmål rätta eller komplettera sådana personuppgifter om den registrerade som är oriktiga eller bristfälliga med tanke på ändamålet med behandlingen.

Den registeransvarige ska på eget initiativ eller på yrkande av den registrerade utan obefogat dröjsmål radera personuppgifter om den registrerade, om behandlingen av dem står i strid med bestämmelserna i 4–7 eller 11 §. I stället för radering ska den registeransvarige dock begränsa behandlingen om

1. den registrerade bestrider personuppgifternas korrekthet och det inte kan fastställas huruvida de är korrekta, eller
2. personuppgifterna måste sparas som bevisning.

Om behandlingen har begränsats med stöd av 2 mom. 1 punkten, ska den registeransvarige innan begränsningen av behandlingen upphävs informera den registrerade om detta.

26 §

Vägran att godkänna den registrerades yrkande

Om inte den registeransvarige godkänner den registrerades yrkande på rättelse, komplettering eller radering av personuppgifter eller begränsning av behandlingen av dem, ska den registeransvarige skriftligen informera den registrerade om vägran och skälen till vägran. Skyldigheten att tillhandahålla information om grunderna för vägran kan helt eller delvis lämnas obeaktad till den del det är nödvändigt av de skäl som anges i 28 §.

Den registeransvarige ska informera den registrerade om rätten att lämna in klagomål till Dataskyddsmyndigheten och uppge myndighetens kontaktuppgifter, om eventuell rätt att i enlighet med 29 § utöva de rättigheter som avses i 25 § via Dataskyddsmyndigheten samt om möjligheten att utnyttja andra rättsmedel.

27 §

Den registeransvariges skyldighet att informera om rättelse, radering eller begränsning av behandling

Den registeransvarige ska anmäla varje rättelse av oriktiga personuppgifter till den myndighet från vilken de oriktiga personuppgifterna kommer.

Om personuppgifter har rättats eller raderats eller behandlingen av dem har begränsats, ska den registeransvarige informera de mottagare om saken till vilka den registeransvarige har lämnat ut uppgifterna.

28 §

Begränsning av de registrerades rättigheter

De registrerades rättigheter kan begränsas på det sätt som anges i 24 § 1 mom., 26 § 1 mom. och 35 §, om det med beaktande av den registrerades rättigheter är en proportionell och nödvändig åtgärd i syfte att

1. undvika menlig inverkan på förebyggande, förhindrande, avslöjande, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
2. trygga andra undersökningar, utredningar eller motsvarande förfaranden hos myndigheter,
3. skydda den allmänna säkerheten,

4. skydda den nationella säkerheten, eller
5. skydda andra personers rättigheter.

29 §

Utövande av rättigheter via Dataskyddsmyndigheten

Den registrerade har rätt att be Dataskyddsmyndigheten kontrollera lagenligheten i personuppgifter och behandlingen av dem, om den registrerades rätt till insyn har skjutits upp, begränsats eller vägrats med stöd av denna eller någon annan lag eller om den registeransvarige inte godkänner den registrerades yrkande på rättelse, komplettering, radering eller begränsning av personuppgifterna.

Om den registrerade utövar sin rätt enligt 1 mom., ska Dataskyddsmyndigheten inom en rimlig tid informera den registrerade om vilka åtgärder myndigheten har vidtagit. Dataskyddsmyndigheten ska också informera den registrerade om dennes rätt att utnyttja rättsmedel.

30 §

Främjande av den registrerades möjligheter att utöva sina rättigheter samt avgiftfria åtgärder

Den registeransvarige ska främja den registrerades möjligheter att utöva de rättigheter som avses i detta kapitel. Alla meddelanden och all information om behandling av personuppgifter som lämnas till den registrerade ska tillhandahållas i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk.

Meddelanden och information som ska ges den registrerade enligt denna lag samt behandlingen av begäranden som den registrerade framställt i enlighet med denna lag är avgiftsfria för den registrerade. Om den registrerades begäranden på grund av deras repetitiva natur eller av någon annan orsak är uppenbart orimliga eller ogrundade, får den registeransvarige dock för åtgärden ta ut en avgift enligt vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

Om den registeransvarige på det sätt som avses i 2 mom. tar ut en avgift, ska denne vid behov visa att begäran är uppenbart orgrundad eller orimlig.

5 kap.

Informationssäkerhet

31 §

Skydd av personuppgifter

Den registeransvarige och registerföraren ska genom tekniska och organisatoriska åtgärder skydda personuppgifterna för att säkerställa en sådan informationssäkerhetsnivå som kan anses nödvändig på grund av den risk för den registrerades rättigheter som behandlingen medför. Personuppgifterna ska särskilt skyddas för obehörig behandling och mot förlust, förstörelse eller skada genom olyckshändelse. Åtgärderna ska planeras och genomföras med beaktande av

1. den senaste tekniska utvecklingen,
2. kostnaderna för att genomföra åtgärderna,
3. behandlingens art, omfattning, sammanhang och ändamål, och
4. riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter.

32 §

Skydd av personuppgifter vid automatiserad behandling

När det gäller automatiserad behandling ska den registeransvarige eller registerföraren utöver vad som förutsätts i 31 §, efter en bedömning av riskerna, vidta åtgärder i syfte att

1. vägra varje obehörig person åtkomst till den utrustning som används för behandling,
2. förhindra obehörig läsning, kopiering, ändring eller radering av datamedier,
3. förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter,
4. förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring,
5. säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras nyttjanderätt,

6. säkerställa att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring,
7. säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes,
8. förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av data-medier,
9. säkerställa att de system som används kan återställas vid störningar,
10. säkerställa att systemet fungerar, att funktionsfel rapporteras och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet.

33 §

Registerförarens skyldighet att anmäla en personuppgiftsincident

Registerföraren ska efter att ha fått vetskap om en personuppgiftsincident utan obefogat dröjsmål anmäla incidenten till den registeransvarige.

34 §

Den registeransvariges skyldighet att anmäla en personuppgiftsincident till Dataskyddsmyndigheten

Den registeransvarige ska anmäla en personuppgiftsincident till Dataskyddsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för den registrerades rättigheter.

Den registeransvarige ska göra anmälan utan obefogat dröjsmål och om möjligt inom 72 timmar efter att ha fått vetskap om incidenten. Om anmälan till Dataskyddsmyndigheten görs senare än så, ska orsakerna till förseningen nämnas i anmälan.

Den registeransvarige ska bevara uppgifter om personuppgiftsincidenter och omständigheter i samband med dem, deras effekter och de korrigerande åtgärder som vidtagits.

35 §

Den registeransvariges skyldighet att anmäla en personuppgiftsincident till den registrerade

Den registeransvarige ska utan obefogat dröjsmål anmäla en personuppgiftsincident till den registrerade, om personuppgiftsincidenten sannolikt kommer att medföra en betydande risk för den registrerades rättigheter. Anmälningssplikt föreligger dock inte, om

1. lämpliga tekniska och organisatoriska skyddsåtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten,
2. den registeransvarige efter incidenten har vidtagit åtgärder för att säkerställa att en risk för den registrerades rättigheter sannolikt inte kommer att uppstå.

Den registeransvarige kan i stället för en anmälan till den registrerade upplysa om personuppgiftsincidenten genom information till allmänheten, om en anmälan till den registrerade skulle kräva en orimlig ansträngning.

Anmälan till den registrerade kan skjutas upp, begränsas eller utelämnas, om de förutsättningar som anges i 28 § uppfylls.

36 §

Den registeransvariges skyldighet att anmäla en personuppgiftsincident till en annan registeransvarig

Den registeransvarige ska utan obefogat dröjsmål anmäla en personuppgiftsincident till registeransvariga i Finland eller i andra EU-medlemsstater, om incidenten gäller personuppgifter som har överförts av eller till den registeransvarige i fråga.

37 §

Innehållet i anmälan om en personuppgiftsincident

En anmälan till Dataskyddsmyndigheten och till registeransvariga i Finland eller i andra EU-medlemsstater ska innehålla en beskrivning av personuppgiftsincidentens art. Beskrivningen ska om möjligt inbegripa de kategorier av och det ungefärliga antal registrerade som berörs samt de kategorier av personuppgifter och det ungefärliga antal personuppgiftsposter som berörs.

En anmälan som ges den registrerade ska innehålla en beskrivning av personuppgiftsincidentens art.

Av de anmälningar som avses i 1 och 2 mom. ska ytterligare framgå

1. namnet på och kontaktuppgifterna för den dataskyddsansvarige eller en annan kontaktpunkt där mer information kan erhållas,
2. de sannolika konsekvenserna av personuppgiftsincidenten, och
3. de åtgärder som den registeransvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten och vid behov åtgärder för att mildra dess negativa effekter.

Den information som ges Dataskyddsmyndigheten och registeransvariga i Finland eller i andra EU-medlemsstater får tillhandahållas i omgångar till den del det inte är möjligt att tillhandahålla informationen samtidigt.

6 kap.

Dataskyddsansvarig

38 §

Utnämning av dataskyddsansvarig

Den registeransvarige ska utnämna en dataskyddsansvarig som har tillräcklig sakkunskap om lagstiftning och praxis i fråga om behandling av personuppgifter samt förmåga att sköta de uppgifter som avses i 40 §. En enda dataskyddsansvarig får utnämnas för flera behöriga myndigheter, om det är motiverat med hänsyn till myndigheternas organisationsstruktur och storlek.

Den registeransvarige ska meddela Dataskyddsmyndigheten den dataskyddsansvariges kontaktuppgifter.

39 §

Den dataskyddsansvariges ställning

Den registeransvarige ska på ett korrekt sätt och i god tid se till att den dataskyddsansvarige deltar i alla frågor som rör skyddet av personuppgifter.

Den registeransvarige ska ge den dataskyddsansvarige verksamhetsförutsättningar att sköta de uppgifter som denne ansvarar för enligt 40 § samt ge tillgång till personuppgifter och behandlingsförfaranden.

40 §

Den dataskyddsansvariges uppgifter

Den dataskyddsansvarige ska

1. ge den registeransvarige och hos denne anställda registerförare råd i frågor som gäller skydd av personuppgifter,
2. övervaka att de bestämmelser som gäller behandling av personuppgifter och den registeransvariges förfaranden för behandling av personuppgifter iakttas,
3. på begäran ge råd om konsekvensbedömningen avseende dataskydd och övervaka att den genomförs i enlighet med 20 §,
4. samarbeta med Dataskyddsmyndigheten och fungera som kontaktpunkt för den i frågor som gäller behandling av personuppgifter.

Den dataskyddsansvariges uppgifter gäller inte sådan behandling av personuppgifter som domstolarna, justitiekanslern i statsrådet och riksdagens justitieombudsman utför i samband med rättskipningsuppgifter.

7 kap.

Överföringar av personuppgifter till tredjeländer och internationella organisationer

41 §

Allmänna principer för överföring av personuppgifter

De behöriga myndigheterna får överföra personuppgifter till ett tredjeland eller en internationell organisation endast om de övriga bestämmelser som är tillämpliga på behandling av personuppgifter enligt denna lag iakttas och om

1. överföringen är nödvändig för det ändamål som avses i 1 § 1 mom. i denna lag,
2. personuppgifterna överförs till en registeransvarig i ett tredjeland eller till en internationell organisation som är behörig att behandla personuppgifter för det ändamål som avses i 1 § 1 mom.,

3. det finns ett i artikel 36 i dataskyddsdirektivet avsett giltigt beslut av Europeiska kommissionen (*kommissionen*) om adekvat skyddsnivå eller, om inget sådant beslut har antagits, när lämpliga skyddsåtgärder föreligger i enlighet med 42 §, eller när undantag för särskilda situationer gäller i enlighet med 43 §.

Om personuppgifter har erhållits från en annan EU-medlemsstat, är en ytterligare förutsättning för överföring att medlemsstaten i fråga har gett tillstånd till överföringen. Överföringar som görs utan ett sådant tillstånd är tillåtna endast om överföringen är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i ett land eller mot en EU-medlemsstats väsentliga intressen och tillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska informeras om överföringen utan dröjsmål.

Om den behöriga myndighet som gjorde den ursprungliga överföringen vid vidare överföring till ett annat tredjeland eller en internationell organisation godkänner vidareöverföringen med iakttagande av bestämmelserna i 1 och 2 mom. och med beaktande av alla relevanta omständigheter, inbegripet brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i tredjelandet till vilket eller den internationella organisationen till vilken personuppgifterna förts vidare.

42 §

Överföring på basis av lämpliga skyddsåtgärder

Om kommissionen inte har antagit ett beslut som avses i 41 § 1 mom. 3 punkten, kan personuppgifter överföras till ett tredjeland eller en internationell organisation, om de övriga förutsättningar som anges i 41 § uppfylls, och om

1. lämpliga skyddsåtgärder för personuppgifter fastställs i en rättsligt bindande handling, eller
2. den registeransvarige efter att ha bedömt alla omständigheter kring en överföring av personuppgifter drar slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

Den registeransvarige ska informera Dataskyddsmyndigheten om de kategorier av överföringar som gjort på basis av 1 mom. 2 punkten. Uppgifter om överföringarna ska bevaras och på begäran göras tillgängliga för Dataskyddsmyndigheten. De uppgifter som bevaras ska innehålla information om datum och tidpunkt för överföringarna, den mottagande behöriga myndigheten, grunderna för överföringarna och de personuppgifter som har överförts.

43 §

Undantag i särskilda situationer

Om kommissionen inte har antagit ett beslut som avses i 41 § 1 mom. 3 punkten och de förutsättningar för uppgiftsöverföring som anges i 42 § inte uppfylls, kan personuppgifter överföras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig

1. för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person,
2. för att skydda den registrerades berättigade intressen,
3. för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en EU-medlemsstat eller ett tredjeland, eller
4. i enskilda fall för de ändamål som nämns i 1 § 1 mom. eller för att uppgöra, framföra eller försvara rättsliga anspråk som hänför sig till dem.

Personuppgifter får dock inte överföras med stöd av 1 mom. 4 punkten, om den berörda registrerades rättigheter ska anses väga tyngre än det allmänna intresset.

Uppgifter om överföringar som baserar sig på 1 mom. ska bevaras och på begäran göras tillgängliga för Dataskyddsmyndigheten. De uppgifter som bevaras ska innehålla information om datum och tidpunkt för överföringen, den mottagande behöriga myndigheten, grunderna för överföringen och de personuppgifter som har överförts.

44 §

Överföring av personuppgifter till enskilda mottagare och andra mottagare i tredjeländer

En behörig myndighet som avses i 3 § 7 a-punkten får trots vad som föreskrivs i 41 § 1 mom. 2 punkten i enskilda fall överföra personuppgifter direkt till enskilda mottagare och andra mottagare som är etablerade i tredjeländer, om de övriga bestämmelserna i denna lag iakttas och om

1. överföringen är nödvändig för att en överförande behörig myndighet ska kunna utföra de uppgifter som den ansvarar för enligt 1 § 1 mom.,
2. den behöriga myndighet som överför uppgifterna anser att ingen av den berörda registrerades rättigheter väger tyngre än det allmänna intresse som gör överföringen nödvändig i det aktuella fallet,

3. den behöriga myndighet som överför uppgifterna anser att en överföring till en behörig myndighet i tredjelandet på grund av ärendets brådskande natur eller av någon annan orsak är ineffektiv eller olämplig,
4. den myndighet i tredjelandet som är behörig för de ändamål som avses i 1 § 1 mom. utan obefogat dröjsmål har informerats, såvida detta inte är ineffektivt eller olämpligt,
5. den behöriga myndighet som överför uppgifterna har informerat mottagaren om det eller de specifika ändamål för vilka personuppgifterna får behandlas, att behandlingen ska vara nödvändig för dessa ändamål och att uppgifterna inte får behandlas för andra ändamål,
6. överföringen inte strider mot Finlands internationella avtalsförpliktelser.

Den behöriga myndighet som överför uppgifterna ska bevara information om överföringar som utförs med stöd av 1 mom. och informera Dataskyddsmyndigheten om överföringen.

8 kap.

Tillsynsmyndighet

45 §

Dataskyddsmyndigheten

Tillsyn över efterlevnaden av denna lag utövas av Dataskyddsmyndigheten enligt 7§ i dataskyddslagen (_201_).

Bestämmelserna om tillsyn i detta kapitel tillämpas inte på domstolarna, justitiekanslern i statsrådet eller riksdagens justitieombudsman i fråga om verksamhet som hänför sig till rättsskipning.

Dataskyddsmyndigheten ska vara oberoende vid utförandet av sina uppgifter enligt denna lag.

46 §

Uppgifter

Dataskyddsmyndigheten ska förutom att utöva tillsyn över efterlevnaden av denna lag

1. öka allmänhetens medvetenhet om risker, lagstiftning, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter,

2. öka den registeransvariges och registerförarens medvetenhet om sina skyldigheter enligt denna lag,
3. på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt denna lag,
4. ge rådgivning vid förhandssamråd enligt 21 §,
5. göra utredningar om efterlevnaden av denna lag,
6. kontrollera att behandling enligt 29 § är laglig,
7. behandla klagomål från en registrerad eller från ett samfund som avses i 55 § 2 mom., och
8. följa sådan teknisk och annan utveckling som påverkar skyddet av personuppgifter,

Dataskyddsmyndigheten ska dessutom bidra till verksamheten i den styrelse som inrättats genom förordning (EU) 2016/679. Dataskyddsmyndigheten ska dock inte föra sådana ärenden till styrelsen som gäller behandling av personuppgifter i samband med verksamhet som avses i 1 § 2 mom.

Dataskyddsmyndighetens åtgärder är avgiftsfria för den registrerade och för den dataskyddsansvarige. Om den registrerades eller den dataskyddsansvariges begäranden dock på grund av deras repetitiva natur eller av någon annan orsak är uppenbart orimliga eller grundade, kan myndigheten

1. ta ut avgift för prestationerna enligt lagen om grunderna för avgifter till staten (150/1992), eller
2. lämna det ärende som begäran gäller utan prövning.

Om Dataskyddsmyndigheten på det sätt som avses i 2 mom. tar ut en avgift eller lämnar ärendet utan prövning, ska myndigheten vid behov visa att begäran är uppenbart ogrundad eller orimlig.

47 §

Rätt till upplysningar

Dataskyddsmyndigheten har trots sekretessbestämmelserna rätt att av den registeransvarige och registerföraren samt dennes företrädare avgiftsfritt få ett i 22 § avsett register över behandlingsåtgärderna, de logguppgifter som avses i 19 § samt de övriga uppgifter som är nödvändiga för att myndigheten ska kunna sköta sina uppgifter.

Dataskyddsmyndigheten har rätt att av den registeransvarige och registerföraren få en utredning om omständigheter som myndigheten behöver för att kunna sköta sina uppgifter.

48 §

Rätt att göra inspektioner

Dataskyddsmyndigheten får göra inspektioner i den registeransvariges och registerförarens lokaler, om en inspektion behövs för tillsynen över efterlevnaden av denna lag. Inspektioner får inte utföras i utrymmen som används för boende av permanent natur. Vid inspektion ska bestämmelserna i 39 § i förvaltningslagen (434/2003) iakttas.

Polisen är skyldig att vid behov ge Dataskyddsmyndigheten handräckning för en inspektion som avses i 1 mom.

49 §

Anlitande av sakkunniga

Dataskyddsmyndigheten får i samband med en inspektion som avses i 48 § anlita utomstående sakkunniga som hjälp. Dataskyddsmyndigheten kan till sakkunnig utse en person som gett sitt samtycke till uppdraget och som besitter sakkunskap av betydelse med tanke på skötseln av Dataskyddsmyndighetens uppgift.

På en sakkunnig som avses i 1 mom. tillämpas bestämmelserna om tjänsteansvar när den sakkunnige utför uppgifter som avses i denna lag.

50 §

Åtgärder

Dataskyddsmyndigheten kan inom tillämpningsområdet för denna lag

1. ge den registeransvarige handledning vid det förfarande för förhandssamråd som avses i 21 §,
2. informera den registeransvarige eller registerföraren om påstådda överträdelser av bestämmelserna i denna lag,
3. utfärda varningar till den registeransvarige eller registerföraren om att planerade behandlingar kan stå i strid med denna lag,
4. ge den registeransvarige eller registerföraren en anmärkning, om denne behandlat personuppgifter i strid med lag,
5. beordra den registeransvarige eller registerföraren att iaktta den registrerades begäran om utövande av sina rättigheter enligt denna lag,

6. beordra den registeransvarige att informera den registrerade om en personuppgiftsincident,
7. införa ett tillfälligt eller bestående förbud eller någon annan tillfällig eller bestående begränsning av behandlingen,
8. bestämma att överföring av uppgifter ska avbrytas till en mottagare eller en internationell organisation i ett tredjeland,
9. beordra rättelse eller radering av personuppgifter eller begränsning av behandlingen eller andra åtgärder i samband med dem på basis av 25 §,
10. beordra den registeransvarige eller registerföraren att se till att uppgiftsbehandlingen är förenlig med bestämmelserna i denna lag, vid behov på ett bestämt sätt och inom en rimlig tid.

51 §

Vite

Dataskyddsmyndigheten kan förena ett beslut som avses i 50 § 5–10 punkten och sådan rätt till upplysningar som avses i 47 § med vite. Bestämmelser om föreläggande och utdömande av vite finns i viteslagen (1113/1990).

52 §

Hörande av Dataskyddsmyndigheten

Dataskyddsmyndigheten kan på eget initiativ eller på begäran yttra sig i frågor som hänför sig till sådan behandling av personuppgifter som avses i 1 §.

Dataskyddsmyndigheten ska beredas tillfälle att bli hörd vid beredningen av lagstiftnings- eller förvaltningsreformer som gäller sådan behandling av personuppgifter som avses i 1 §.

Domstolen ska vid behandlingen av ett ärende som gäller tillämpningen av denna lag bereda Dataskyddsmyndigheten möjlighet att bli hörd. Åklagaren ska bereda Dataskyddsmyndigheten tillfälle att bli hörd i ärenden som gäller ett förfarande som står i strid med denna lag.

53 §

Ömsesidigt bistånd

Dataskyddsmyndigheten ska avgiftsfritt ge motsvarande tillsynsmyndighet i en annan EU-medlemsstat de personuppgifter som denne oundgängligen behöver i sin tillsyns-

uppgift samt andra behövliga uppgifter, och vid behov även annars bistå denne vid utövandet av tillsynen. Dataskyddsmyndigheten ska vidta också andra behövliga åtgärder för att säkerställa ett effektivt samarbete.

Dataskyddsmyndigheten ska besvara en begäran från en tillsynsmyndighet som avses i 1 mom. utan obefogat dröjsmål och inte senare än en månad efter det att den tagit emot begäran.

9 kap.

Rättsskydd

54 §

Rapportering av överträdelser

Den behöriga myndigheten ska ha rutiner som gör det möjligt att konfidentiellt rapportera en misstanke om överträdelser av bestämmelserna i denna lag. Förfarandet ska innehålla lämpliga och tillräckliga åtgärder för att ordna en korrekt behandling av rapporterna. Rapporteringsförfarandet ska dessutom innehålla anvisningar som tryggar skyddet för rapportörens identitet.

Den behöriga myndigheten ska bevara behövlig information som gäller den rapport som avses i 1 mom. Informationen ska avföras fem år efter rapporteringen, om den inte fortfarande behövs för en brottsutredning, en pågående rättegång eller en myndighetsundersökning eller för att trygga de rättigheter som rapportören eller den som är föremål för rapporten har. Senast tre år efter den föregående undersökningen ska behovet av fortsatt bevarande undersökas. En anteckning ska göras om undersökningen.

Om en fysisk person till den behöriga myndigheten har rapporterat en misstanke om överträdelse av bestämmelserna i denna lag, ska rapportörens identitet sekretessbäggas, om det på basis av omständigheterna kan antas medföra olägenhet för rapportören att hans eller hennes identitet röjs.

Bestämmelserna om en parts rätt till information i lagen om offentlighet i myndigheternas verksamhet tillämpas inte i en situation som avses i 3 mom., om det skulle äventyra rapportörens i säkerhet, intressen eller rättigheter att hans eller hennes identitet röjs.

55 §

Klagomål till Dataskyddsmyndigheten

Registrerade personer har rätt att lämna in ett klagomål till Dataskyddsmyndigheten, om de registrerade anser att behandling som avser dem står i strid med denna lag.

Klagomålet kan med den registrerades samtycke lämnas in till Dataskyddsmyndigheten för behandling också av ett allmännyttigt samfund som främjar skyddet av personuppgifter.

56 §

Behandling av klagomål

Dataskyddsmyndigheten prövar klagomålet samt informerar inom rimlig tid den som inlämnat det om hur behandlingen fortskrider och om resultatet. Myndigheten tar dock inte ett mål som är anhängigt i domstol till prövning.

Om Dataskyddsmyndigheten i ett ärende om tillsyn över efterlevnaden av denna lag som är anhängigt hos myndigheten anser det behövt att utreda huruvida ett i 41 § 1 mom. 3 punkten avsett beslut av Europeiska kommissionen om adekvat skyddsnivå är förenligt med dataskyddsdirektivet, kan myndigheten genom en ansökan föra tillsynsärendet till Helsingfors förvaltningsdomstol för avgörande.

57 §

Ändringssökande

Beslut som Dataskyddsmyndigheten har fattat får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Ett beslut av förvaltningsdomstolen i ett ärende som avses i 56 § 2 mom. får överklagas genom besvär hos högsta förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen.

Över andra beslut av förvaltningsdomstolen får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd. Även Dataskyddsmyndigheten får söka ändring i ett sådant beslut av förvaltningsdomstolen.

I Dataskyddsmyndighetens beslut kan det bestämmas att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.

10 kap.

Särskilda bestämmelser

58 §

Skadestånd

Den registeransvarige är skyldig att ersätta den ekonomiska skada eller annan skada som tillfogats den registrerade eller någon annan person av att personuppgifter har behandlats i strid med denna lag.

Bestämmelser om rätten till skadestånd finns i övrigt i skadeståndslagen (412/1974).

59 §

Straffbestämmelser i strafflagen

Bestämmelser om straff för dataskyddsbrott finns i 38 kap. 9 § i strafflagen (39/1889). Bestämmelser om straff för kränkning av kommunikationshemlighet och för grov kränkning av kommunikationshemlighet finns i 38 kap. 3 och 4 § samt bestämmelser om straff för dataintrång och för grovt dataintrång i 38 kap. 8 och 8 a §. Straff för brott mot den tystnadsplikt som anges i 60 § i denna lag utdöms enligt 38 kap. 1 eller 2 § i strafflagen, om inte gärningen ska bestraffas enligt 40 kap. 5 § i strafflagen eller om inte strängare straff för den föreskrivs någon annanstans i lag.

60 §

Tystnadsplikt

Den som har deltagit i behandlingen av personuppgifter får inte obehörigen för tredje man röja de uppgifter som han eller hon på detta sätt har fått kännedom om.

11 kap.

Ikraftträdande- och övergångsbestämmelser

61 §

Ikraftträdande

Denna lag träder i kraft den 6 maj 2018.

62 §

Övergångsbestämmelser

Automatiserade behandlingssystem som har inrättats före den 6 maj 2016 ska bringas i överensstämmelse med 19 § senast den 6 maj 2023.

Vad som i denna lag föreskrivs om Dataskyddsmyndigheten tillämpas efter det att dataskyddslagen (/) har trätt i kraft. Tillsyn över efterlevnaden av denna lag utövas fram till dess av dataombudsmannen enligt vad som föreskrivs i personuppgiftslagen.

2.

**Lag
om ändring av 1 och 6 § i straffregisterlagen**

I enlighet med riksdagens beslut

ändras i straffregisterlagen (770/1993) 1 § 1 mom. och 6 § 8 mom., sådana de lyder, 1 § 1 mom. i lag 1093/1999 och 6 § 8 mom. i lag 215/2012, som följer:

1 §

Straffregistrets ändamål och innehåll

Registeransvarig i fråga om straffregistret är Rättsregistercentralen.

6 §

— — —

Den som har rätt att teckna en juridisk persons namn har rätt att på begäran få ett i 5 § 1 mom. avsett straffregisterutdrag som gäller den juridiska personen.

3.

Lag

om ändring av lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen

I enlighet med riksdagens beslut

ändras i lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen (214/2012) 4 § 3 mom., 8 och 13 §, som följer:

4 §

Förhållande till andra lagar och internationella förpliktelser

— — —

Om inte något annat föreskrivs i denna lag eller i någon annan lag tillämpas lagen om offentlighet i myndigheternas verksamhet (621/1999) på sekretess för samt utlämnande och skydd av personuppgifter samt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) på annan behandling av personuppgifter.

8 §

Lagringsregistrets syfte

Registeransvarig i fråga om lagringsregistret är Rättsregistercentralen. Lagringsregistret förs i syfte att lagra uppgifter så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag enligt vad som föreskrivs i denna lag.

13 §

Kontrollrätt

I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt.

4.

Lag om ändring av lagen om justitieförvaltningens riksomfattande informationssystem

I enlighet med riksdagens beslut

upphävs i lagen om justitieförvaltningens riksomfattande informationssystem (372/2010) 18 § 2 mom., och

ändras 2 § 1 mom., 10 § 2 mom. och 19 § som följer:

2 §

Förhållande till annan lagstiftning

Utöver vad som föreskrivs i denna lag, gäller i fråga om utlämnande av uppgifter ur justitieförvaltningens riksomfattande informationssystem och i fråga om de i systemet införda uppgifternas offentlighet vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt i fråga om behandling av personuppgifter vad som föreskrivs i förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, i dataskyddslagen (/) samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

10 §

Personuppgifter som ska registreras i informationssystemet

I registret över avgöranden och meddelanden om avgöranden får det om fysiska personer i partsställning antecknas endast sådana känsliga uppgifter som avses i artikel 9 i allmänna dataskyddsförordningen avseende behandling av personuppgifter och som ska registreras i domstolars diarie- eller andra dokumentregister eller som framgår av en justitieförvaltningsmyndighets avgörande och behövs för verkställighet av

en dom, för registrering i myndighetsregister eller för fullgörande av andra justitieförvaltningsmyndigheters lagstadgade uppgifter.

19 §

Rätt till insyn och rättelse av uppgifter

I fråga om den registrerades rätt till insyn och rätt att få sina uppgifter korrigerade eller kompletterade föreskrivs särskilt.

5.

Lag
om ändring av 46 och 49 § i lagen om verkställighet av böter

I enlighet med riksdagens beslut

upphävs i lagen om verkställighet av böter (672/2002) 49 §, och

ändras 46 § 3 mom. som följer:

46 §

Ändamålet med bötesregistret och behandlingen av registeruppgifterna

— — —

Utöver vad som föreskrivs i denna lag eller i någon annan lag gäller i fråga om rätten att ta del av myndigheternas offentliga handlingar samt om tystnadsplikt för myndigheter, om handlingssekretess samt andra för skyddande av allmänna och enskilda intressen nödvändiga begränsningar av rätten att ta del av en handling vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt om annan behandling av personuppgifter vad som föreskrivs i förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, i dataskyddslagen (/) samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

6.

**Lag
om ändring av lagen om behandling av personuppgifter vid
Brottspåföljdsmyndigheten**

I enlighet med riksdagens beslut

ändras i lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten (1069/2015) 1, 30 och 31 § samt 33 § 1 mom. som följer:

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av personuppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999) och på annan behandling av personuppgifter förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, dataskyddslagen (/) samt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

30 §

Information om behandling av uppgifter

Den registeransvarige ska i enlighet med vad som föreskrivs i allmänna dataskyddsförordningen och dataskyddslagen informera den registrerade om behandling av uppgifter. Undantag från informationsplikten kan dock göras om det är nödvändigt för ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten.

31 §

Inskränkningar i rätten till insyn

Utöver vad som föreskrivs i allmänna dataskyddsförordningen, dataskyddslagen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten kan den registrerades rätt till insyn begränsas, om utövande av rätten till insyn på sannolika grunder kan leda till ett allvarligt hot mot ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten eller mot säkerheten för en anställd vid Brottspåföljdsmyndigheten eller för någon annan. Den registrerade har inte rätt till insyn i uppgifter i säkerhetsregistret eller i de uppgifter om målsägande enligt 7 § 1 mom. 10 punkten i denna lag som ingår i övervaknings- och verksamhetsregistret.

Dataskyddsmyndigheten kan på begäran av den registrerade kontrollera att de uppgifter om den registrerade som avses i 1 mom. är lagenliga.

33 §

Bevaring av uppgifter som konstaterats vara oriktiga

Oberoende av vad som i allmänna dataskyddsförordningen, dataskyddslagen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten föreskrivs om rättelse av oriktiga uppgifter i ett register får en oriktig uppgift bevaras i samband med den rättade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en anställd vid Brottspåföljdsmyndigheten. En sådan uppgift får användas endast i det syfte som här avses.

37 §

Straffbestämmelser

Till straff för dataskyddsbrott döms enligt 38 kap. 9 § i strafflagen och till straff för dattintrång i personregister enligt 38 kap. 8 § i strafflagen.

7.

Lag
om ändring av 1 kap. 27 och 28 § i utsökningsbalken

I enlighet med riksdagens beslut

ändras i utsökningsbalken (705/2007) 1 kap. 27 § 1 mom. och 28 § som följer:

27 §

Rätt att behandla uppgifter

Bestämmelser om behandlingen av personuppgifter som har samlats in för utsökningsregistret och som har förts in i det finns förutom i denna lag i allmänna dataskyddsförordningen, i dataskyddslagen (/) samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

— — —

28 §

Inskränkningar i de registrerades rätt till insyn

Bestämmelser om de registrerades rätt till insyn finns i allmänna dataskyddsförordningen samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Om rätten till insyn skulle försvåra verkställigheten avsevärt, kan utövandet av rätten till insyn skjutas upp till behövliga delar tills behövliga utmätningar eller andra verkställighetsåtgärder har utförts och egendomen har tagits om hand av utmätningsmannen, dock högst sex månader från begäran om rätt till insyn.

PARALLELLTEXT

2.

Lag om ändring av 1 och 6 § i straffregisterlagen

I enlighet med riksdagens beslut

ändras i straffregisterlagen (770/1993) 1 § 1 mom. och 6 § 8 mom., sådana de lyder, 1 § 1 mom. i lag 1093/1999 och 6 § 8 mom. i lag 215/2012, som följer:

Gällande lydelse

1 §

Vid *rättsregistercentralen* förs straffregister enligt vad som bestäms i denna lag.

— — —

6 §

I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt. Den som antecknats i straffregistret har dessutom rätt att på begäran få veta till vem och för vilket ändamål det under det senaste året har lämnats ut uppgifter om honom eller henne ur ett sådant register som förs med hjälp av automatisk databehandling. Den som har rätt att teckna en juridisk persons namn har, oberoende av det sätt på vilket registret förs, motsvarande kontrollrätt och rätt att få information för den juridiska personens räkning samt rätt att få ett straffregisterutdrag som gäller den juridiska personen.

Föreslagen lydelse

1 §

Registeransvarig i fråga om straffregistret är Rättsregistercentralen.

— — —

6 §

Den som har rätt att teckna en juridisk persons namn har rätt att på begäran få ett i 5 § 1 mom. avsett straffregisterutdrag som gäller den juridiska personen.

3.

Lag **om ändring av lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen**

I enlighet med riksdagens beslut

ändras i lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen (214/2012) 4 § 3 mom., 8 och 13 §, som följer:

Gällande lydelse

4 §

Förhållande till andra lagar och internationella förpliktelser

Om inte något annat bestäms i denna lag eller i någon annan lag tillämpas lagen om offentlighet i myndigheternas verksamhet ([621/1999](#)) på sekretess för samt utlämnande och skydd av personuppgifter samt personuppgiftslagen ([523/1999](#)) på annan behandling av personuppgifter.

8 §

Lagringsregistrets syfte

Rättsregistercentralen ska föra ett lagringsregister. Lagringsregistret förs i syfte att lagra uppgifter så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag enligt vad som föreskrivs i denna lag.

Föreslagen lydelse

4 §

Förhållande till andra lagar och internationella förpliktelser

Om inte något annat föreskrivs i denna lag eller i någon annan lag tillämpas lagen om offentlighet i myndigheternas verksamhet ([621/1999](#)) på sekretess för samt utlämnande och skydd av personuppgifter samt *lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/)* på annan behandling av personuppgifter.

8 §

Lagringsregistrets syfte

Registeransvarig i fråga om lagringsregistret är Rättsregistercentralen. Lagringsregistret förs i syfte att lagra uppgifter så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag enligt vad som föreskrivs i denna lag.

13 §

Kontrollrätt

I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt. *Den som antecknats i lagringsregistret har dessutom rätt att på begäran få veta till vem och för vilket ändamål det under det senaste året har lämnats ut uppgifter om honom eller henne ur ett sådant register som förs med hjälp av automatisk databehandling.*

13 §

Kontrollrätt

I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt.

4.

Lag om ändring av lagen om justitieförvaltningens riksomfattande informationssystem

I enlighet med riksdagens beslut

upphävs i lagen om justitieförvaltningens riksomfattande informationssystem (372/2010) 18 § 2 mom., och
ändras 2 § 1 mom., 10 § 2 mom. och 19 § som följer:

Gällande lydelse

Föreslagen lydelse

2 §

2 §

Förhållande till annan lagstiftning

Förhållande till annan lagstiftning

Om inte något annat föreskrivs i denna lag, gäller i fråga om utlämnande av uppgifter ur justitieförvaltningens riksomfattande informationssystem och i fråga om de i systemet införda uppgifternas offentlighet vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet ([621/1999](#)) samt i fråga om annan behandling av personuppgifter som förts in i systemet vad som föreskrivs i personuppgiftslagen ([523/1999](#)).

Utöver vad som föreskrivs i denna lag, gäller i fråga om utlämnande av uppgifter ur justitieförvaltningens riksomfattande informations-system och i fråga om de i systemet införda uppgifternas offentlighet vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet ([621/1999](#)) samt i fråga om behandling av personuppgifter vad som föreskrivs i förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, i dataskyddslagen (/) samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

10 §

10 §

*Personuppgifter som ska registreras i
informationssystemet*

*Personuppgifter som ska registreras i
informationssystemet*

I registret över avgöranden och meddelanden om avgöranden får det om fysiska personer i partsställning antecknas endast sådana enligt 11 § i personuppgiftslagen känsliga uppgifter som ska registreras i domstolars diarie- eller andra dokumentregister eller som framgår av en justitieförvaltningsmyndighets avgörande och behövs för verkställighet av en dom, för registrering i myndighetsregister eller för fullgörande av andra justitieförvaltningsmyndigheters lagstadgade uppgifter.

I registret över avgöranden och meddelanden om avgöranden får det om fysiska personer i partsställning antecknas endast sådana *känsliga uppgifter som avses i artikel 9 i allmänna dataskyddsförordningen* avseende behandling av personuppgifter och som ska registreras i domstolars diarie- eller andra dokumentregister eller som framgår av en justitieförvaltningsmyndighets avgörande och

18 §

Gallring av uppgifter

I fråga om gallring av uppgifter ur rapporterings-, statistik- och arkivsystemet tillämpas vad som föreskrivs i personuppgiftslagen eller bestäms med stöd av den.

behövs för verkställighet av en dom, för registrering i myndighetsregister eller för fullgörande av andra justitieförvaltningsmyndigheters lagstadgade uppgifter.

(upphävs)

19 §

Rätt till insyn och rättelse av uppgifter

En justitieförvaltningsmyndighet behandlar och avgör en registrerades begäran om rätt till insyn och korrigering av uppgifter endast om ärendet har behandlats och avgjorts av myndigheten i fråga och denna myndighet registrerat uppgifterna om ärendet i justitieförvaltningens riksomfattande informationssystem.

Rättsregistercentralen kan överföra en registrerads begäran om rätt till insyn eller rättelse av sina personuppgifter till den justitieförvaltningsmyndighet som har fört in uppgifterna om den registrerade i registret över avgöranden och meddelanden om avgöranden eller i rikssystemet för behandling av diarie- och ärendehanteringssuppgifter.

Utan hinder av vad som i 27 § i personuppgiftslagen föreskrivs om rätten till insyn i register som används för statistik och vetenskaplig forskning har den registrerade rätt till insyn, om Rättsregistercentralen med stöd av 13 § i denna lag har använt uppgifter som överförts till rapporterings-, statistik- och arkivsystemet vid behandling av ärenden som berör den registrerade.

I fråga om registrerades rätt till insyn tillämpas i övrigt vad som föreskrivs i personuppgiftslagen.

19 §

Rätt till insyn och rättelse av uppgifter

I fråga om den registrerades rätt till insyn och rätt att få sina uppgifter korrigerade eller kompletterade föreskrivs särskilt.

5.

Lag

om ändring av 46 och 49 § i lagen om verkställighet av böter

I enlighet med riksdagens beslut

upphävs i lagen om verkställighet av böter (672/2002) 49 §, och

ändras 46 § 3 mom. som följer:

46 §

*Ändamålet med bötesregistret och behandlingen av
registeruppgifterna*

— — —

På behandlingen av uppgifter i bötesregistret tillämpas personuppgiftslagen (523/1999) och i fråga om utlämnande av uppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999), om inte något annat bestäms nedan.

49 §

Ansaret för uppgifterna i bötesregistret

Rättsregistercentralen ansvarar för att de uppgifter som registrerats i bötesregistret är felfria och att användningen av registret är laglig. Den registeransvarige är skyldig att ersätta ekonomisk skada och annan skada som orsakats den registrerade eller någon annan av sådan behandling av uppgifter i bötesregistret som har samband med oriktiga uppgifter eller som annars är lagstridig. Skadeståndslagen (412/1974) tillämpas så som föreskrivs i 47 § 2 mom. personuppgiftslagen

46 §

*Ändamålet med bötesregistret och behandlingen av
registeruppgifterna*

— — —

Utöver vad som föreskrivs i denna lag eller i någon annan lag gäller i fråga om rätten att ta del av myndigheternas offentliga handlingar samt om tystnadsplikt för myndigheter, om handlingssekretess samt andra för skyddande av allmänna och enskilda intressen nödvändiga begränsningar av rätten att ta del av en handling vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt om annan behandling av personuppgifter vad som föreskrivs i förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, i dataskyddslagen (/) samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

(upphävs)

6.

Lag

om ändring av lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten

I enlighet med riksdagens beslut

ändras i lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten (1069/2015) 1, 30 och 31 § samt 33 § 1 mom. som följer:

Gällande lydelse

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av personuppgifter lagen om offentlighet i myndigheternas verksamhet ([621/1999](#)) och på annan behandling av personuppgifter personuppgiftslagen ([523/1999](#)).

30 §

Information om behandling av uppgifter

Den registeransvarige ska i enlighet med vad som föreskrivs i personuppgiftslagen informera den registrerade om behandling av uppgifter. Undantag från informationsplikten kan dock göras om det är nödvändigt för ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten.

Föreslagen lydels

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av personuppgifter lagen om offentlighet i myndigheternas verksamhet ([621/1999](#)) och på annan behandling av personuppgifter förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, dataskyddslagen (/) samt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

30 §

Information om behandling av uppgifter

Den registeransvarige ska i enlighet med vad som föreskrivs i *allmänna dataskyddsförordningen och dataskyddslagen* informera den registrerade om behandling av uppgifter. Undantag från informationsplikten kan dock göras om det är nödvändigt för ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten.

Inskränkningar i rätten till insyn

Utöver vad som föreskrivs i personuppgiftslagen kan den registrerades rätt till insyn begränsas, om utövande av rätten till insyn på sannolika grunder kan leda till ett allvarligt hot mot ordningen och säkerheten i en enhet vid Brottsförhållningsmyndigheten eller mot säkerheten för en anställd vid Brottsförhållningsmyndigheten eller för någon annan. Den registrerade har inte rätt till insyn i uppgifter i säkerhetsregistret eller i de uppgifter om målsägande enligt 7 § 1 mom. 10 punkten i denna lag som ingår i övervaknings- och verksamhetsregistret. [\(8.1.2016/17\)](#)

Dataombudsmannen kan på begäran av den registrerade kontrollera att de uppgifter om den registrerade som avses i 1 mom. är lagenliga.

Bevaring av uppgifter som konstaterats vara oriktiga

Oberoende av vad som i personuppgiftslagens föreskrivs om rättelse av oriktiga uppgifter i ett register får en oriktig uppgift bevaras i samband med den rättade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en anställd vid Brottsförhållningsmyndigheten. En sådan uppgift får användas endast i det syfte som här avses.

Inskränkningar i rätten till insyn

Utöver vad som föreskrivs i *allmänna dataskyddsförordningen, dataskyddslagen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten* kan den registrerades rätt till insyn begränsas, om utövande av rätten till insyn på sannolika grunder kan leda till ett allvarligt hot mot ordningen och säkerheten i en enhet vid Brottsförhållningsmyndigheten eller mot säkerheten för en anställd vid Brottsförhållningsmyndigheten eller för någon annan. Den registrerade har inte rätt till insyn i uppgifter i säkerhetsregistret eller i de uppgifter om målsägande enligt 7 § 1 mom. 10 punkten i denna lag som ingår i övervaknings- och verksamhetsregistret.

Dataskyddsmyndigheten kan på begäran av den registrerade kontrollera att de uppgifter om den registrerade som avses i 1 mom. är lagenliga.

Bevaring av uppgifter som konstaterats vara oriktiga

Oberoende av vad som i *allmänna dataskyddsförordningen, dataskyddslagen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten* föreskrivs om rättelse av oriktiga uppgifter i ett register får en oriktig uppgift bevaras i samband med den rättade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en anställd vid Brottsförhållningsmyndigheten. En sådan uppgift får användas endast i det syfte som här avses.

37 §

Straffbestämmelser

Till straff för personregisterbrott döms enligt 38 kap. 9 § i strafflagen och till straff för dataintrång i personregister enligt 38 kap. 8 § i strafflagen. *Till straff för personregisterförseelse döms enligt 48 § 2 mom. i personuppgiftslagen.*

37 §

Straffbestämmelser

Till straff för *dataskyddsbrott* döms enligt 38 kap. 9 § i strafflagen och till straff för dataintrång i personregister enligt 38 kap. 8 § i strafflagen.

Lag
om ändring av 1 kap. 27 och 28 § i utsökningsbalken

I enlighet med riksdagens beslut

ändras i utsökningsbalken (705/2007) 1 kap. 27 § 1 mom. och 28 § som följer:

27 §

Rätt att behandla uppgifter

På behandlingen av personuppgifter som har samlats in för utsökningsregistret och som har förts in i det tillämpas personuppgiftslagen, om inte något annat föreskrivs nedan.

— — —

28 §

De registrerades rätt till insyn

Om rätten till insyn enligt personuppgiftslagen skulle försvåra verkställigheten avsevärt, kan utövandet av rätten till insyn skjutas upp till behövliga delar tills behövliga utmätningar eller andra verkställighetsåtgärder har utförts och egendomen har tagits om hand av utmätningsmannen, dock högst sex månader från begäran om rätt till insyn.

Har utövandet av rätten till insyn skjutits upp, kan dataombudsmannen utöver vad som föreskrivs någon annanstans, på begäran av den registrerade kontrollera att registrets uppgifter om den registrerade är lagenliga.

27 §

Rätt att behandla uppgifter

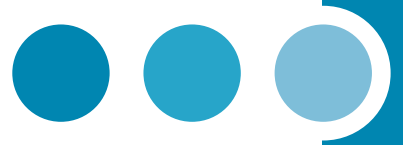
Bestämmelser om behandlingen av personuppgifter som har samlats in för utsökningsregistret och som har förts in i det finns förutom i denna lag i *allmänna dataskyddsförordningen, i dataskyddslagen (/) samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/)*.

— — —

28 §

Inskränkningar i de registrerades rätt till insyn

Bestämmelser om de registrerades rätt till insyn finns i allmänna dataskyddsförordningen samt i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Om rätten till insyn skulle försvåra verkställigheten avsevärt, kan utövandet av rätten till insyn skjutas upp till behövliga delar tills behövliga utmätningar eller andra verkställighetsåtgärder har utförts och egendomen har tagits om hand av utmätningsmannen, dock högst sex månader från begäran om rätt till insyn.



OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

ISSN 1798-7091 (nid.)
ISSN 1798-7105 (PDF)
ISBN 978-952-259-644-4 (nid.)
ISBN 978-952-259-645-1 (PDF)

Oikeusministeriö
PL 25
00023 Valtioneuvosto
www.oikeusministerio.fi

Justitieministeriet
PB 25
00023 Statsrådet
www.justitieministeriet.fi